ELYSIUM

NSATTECH SOLUTIONS

Security Assessment Findings Report

Pentester : Daniel Arconada

Índice

Acuerdo de confidencialidad

Elysium y NSATTECH acuerdan llevar a cabo una actividad de pentesting sobre el activo identificado con la dirección IP 192.168.50.251. El objetivo de esta acción es evaluar el nivel de seguridad del sistema y detectar posibles vulnerabilidades que puedan afectar a la organización desde el día 19 de Septiembre del 2025 hasta el día 24 de Septiembre de 2025.

Ambas partes establecen que toda la información obtenida durante el proceso será tratada con la máxima confidencialidad. Ningún dato, hallazgo o resultado podrá ser compartido con terceros ajenos a las empresas mencionadas.

Los resultados del análisis se utilizarán exclusivamente con fines de mejora de la seguridad de Elysium y no podrán ser difundidos fuera del marco de colaboración existente con NSATTECH.

Información de contacto

Nombre	Contacto	Cargo
Daniel Arconada	d.arconada@elysium.com	Pentester
Jose Miguel	j.miguel@nsattech.com	CISO

Introducción

Se ha llevado a cabo un ejercicio de pentesting sobre el activo designado por NSATTECH con el objetivo de evaluar su nivel de exposición frente a posibles

amenazas. La finalidad principal de esta actividad es reforzar la postura de seguridad de la organización y reducir riesgos operativos que pudieran derivarse de un incidente. Durante la evaluación se identificaron posibles vulnerabilidades y puntos débiles que, en un escenario real, podrían ser aprovechados para comprometer la confidencialidad de la información, obtener accesos no autorizados, interrumpir la disponibilidad de servicios o introducir software malicioso en el entorno.
El presente informe recoge los hallazgos detectados junto con un conjunto de recomendaciones y medidas correctivas orientadas a mejorar la seguridad de los activos de NSATTECH y fortalecer su capacidad de defensa frente a ataques externos.

Alcance

Para este ejercicio de pentesting, la empresa NSATTECH ha escogido auditar el siguiente activo.

Host	Direccion IP
metasploitable2	192.168.50.251

Escenarios excluidos

Quedan expresamente excluidas del alcance del pentesting las pruebas de denegación de servicio (DDoS) y cualquier técnica de ingeniería social (phishing, vishing, smishing o suplantación). Estas restricciones aseguran que la evaluación se limite al activo autorizado, evitando impactos sobre la operativa de negocio, al personal o a terceros no implicados.

Calificación del riesgo

A continuación, se presenta la tabla en la que se ha basado la clasificación de las vulnerabilidades.

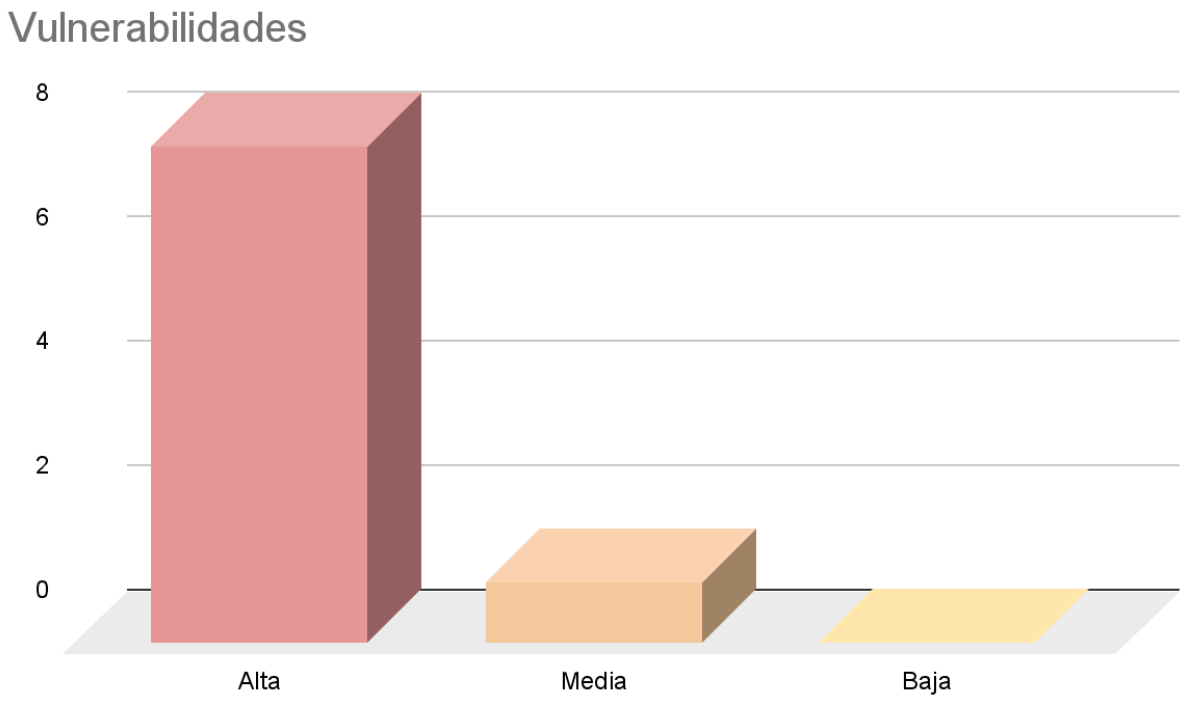
Criticidad	Rango CVSS	Descripción
Alta	8.1-10.0	Supone un riesgo grave que es fácil de explotar. Comienza el proceso de remediación inmediatamente después de que se haya presentado el problema.
Media	6.1-8.0	Supone un riesgo significativo y puede ser explotado. Atiende estos problemas lo antes posible después de que se hayan solucionado los riesgos críticos.
Baja	4.1-6.0	Supone un riesgo importante, pero puede ser difícil de explotar. El pentest recomienda realizar el trabajo de remediación dentro de los 3 meses posteriores a su descubrimiento.

Resumen Ejecutivo

La auditoría de seguridad realizada sobre el activo ha puesto de manifiesto que la empresa se encuentra expuesta a riesgos que podrían tener consecuencias graves en su funcionamiento y reputación. Si no se actúa, existe la posibilidad de pérdida o alteración de información crítica, interrupciones en los procesos internos y afectación directa a clientes y socios. Esto se traduce en costes inesperados para recuperar la

normalidad, gestionar los incidentes y, en caso necesario, cumplir con obligaciones legales, así como en un daño a la confianza que otros depositan en la empresa. En términos prácticos, no abordar estos riesgos ahora significa asumir que cualquier fallo podría convertirse en una crisis que afecte tanto a los resultados económicos como a la credibilidad de la organización. Tomar medidas de forma inmediata es la única manera de proteger los activos clave, asegurar la continuidad de las operaciones y mantener la confianza de quienes dependen de la empresa.

Clasificación de las vulnerabilidades

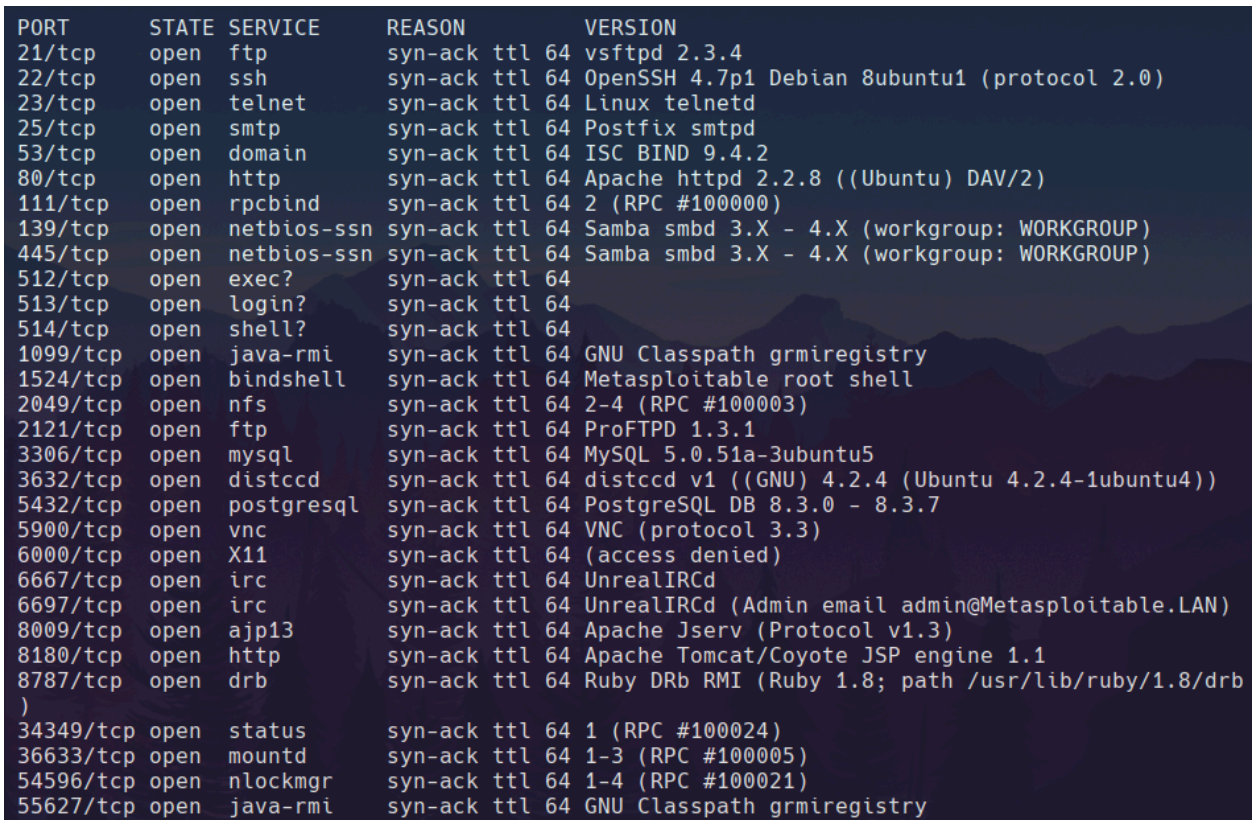


Resumen de vulnerabilidades

ID Vulnerabilidad - Nombre	Recomendación	Impacto	Clasificación CVSS
01 - FTP Backdoor Command Execution	Se recomienda usar una versión más moderna de vsftpd	Alta	10
02 - SQL Injection	Sanitizar la entrada del usuario	Alta	9.5
03 - Upload File Inclusion	Hacer uso de una lista blanca con archivos permitidos	Alta	9.7
04 - Bind Shell	Cerrar este puerto y eliminar cualquier bind shell	Alta	10
05 - PostgreSQL Code Execution	Se recomienda usar una versión más moderna	Alta	9.0
06 - VNC Login	Hacer uso de contraseñas robustas y actualizar la versión	Alta	9.3
07 - IRC Backdoor	Deshabilitar o actualizar el servicio	Alta	9.8
08 - SMB Enumeration	Restringir el uso solamente a redes de confianza	Media	7.8
09 - MySQL Insecure Login	Restringir el acceso y configurar credenciales seguras	Alta	9.8

Análisis Técnico

Vamos a tomar como referencia la siguiente captura en donde referenciamos los puertos encontrados y explotados a través de un escáner de red con nmap al activo dado.



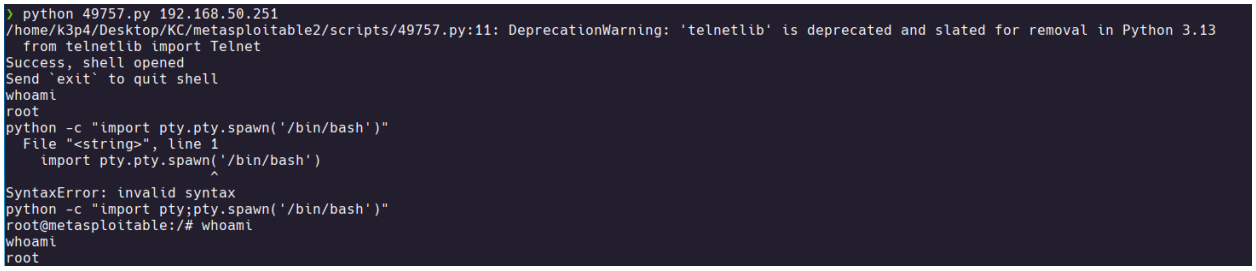
```
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?       syn-ack ttl 64
513/tcp   open  login?      syn-ack ttl 64
514/tcp   open  shell?      syn-ack ttl 64
1099/tcp  open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack ttl 64 (access denied)
6667/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
6697/tcp  open  irc         syn-ack ttl 64 UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb
)
34349/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
36633/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
54596/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
55627/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
```

01 - FTP Backdoor Command Execution

Se ha encontrado en el puerto 21 cuyo protocolo es ftp con versión vsftpd 2.3.4 la cual un CVE 2011-2523. Esta vulnerabilidad abre un backdoor en el puerto 6200. Se consigue a través de una llamada con telnet al puerto 21 e introduciendo un USER y un PASS aleatorios encodeado en ascii. Esto es lo que genera el backdoor y ya podríamos

conectarnos con telnet al puerto 6200 obteniendo una shell como root.

Prueba de concepto :



Recomendación : Se aconseja a la empresa NSATTECH que

- Actualice la versión de este servicio si es que es imprescindible.
- Restringir el uso del servicio a direcciones IP autorizadas por firewall
- Sustituir el servicio por uno más seguro como es SFTP

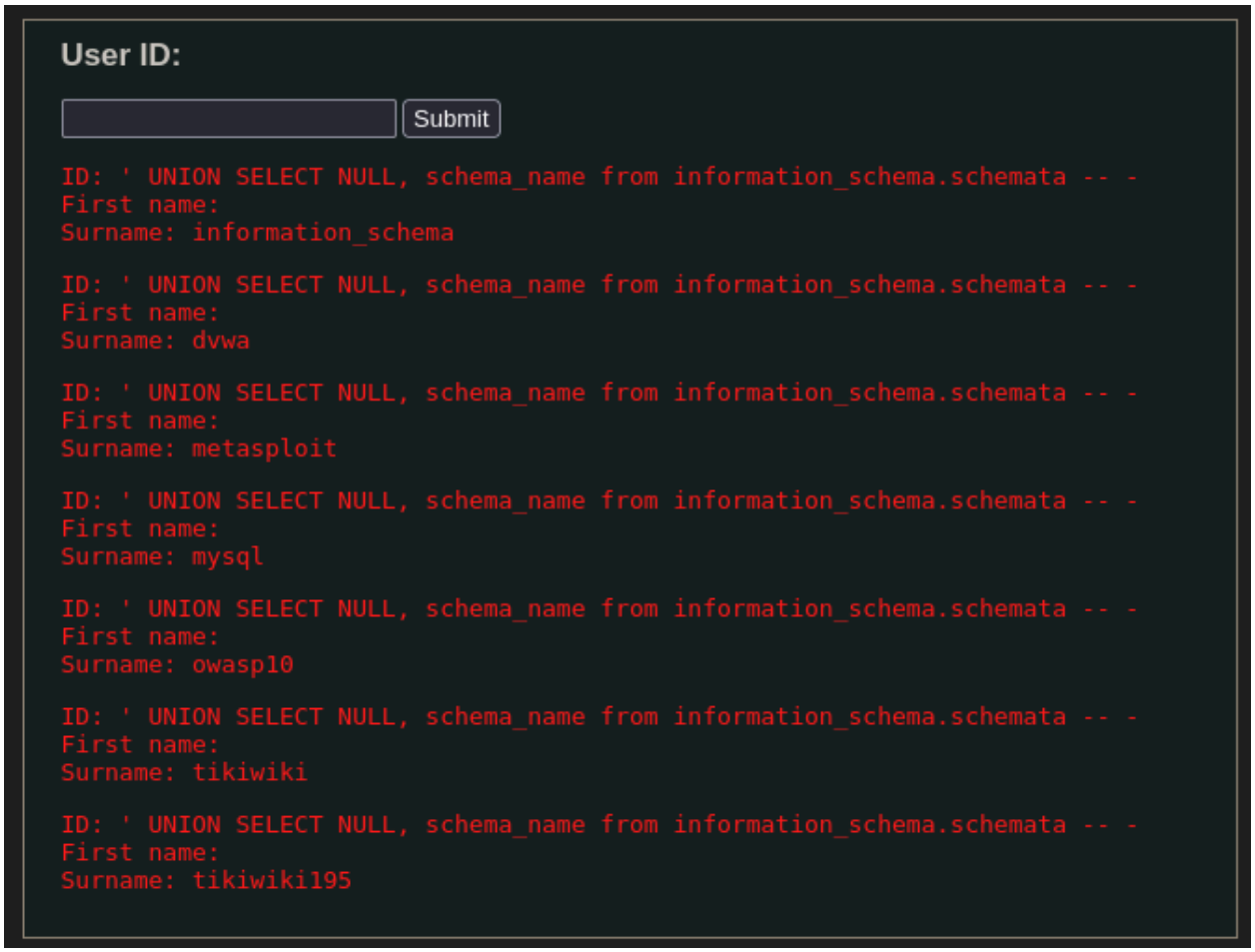
Referencia :

https://hackviser.com/tactics/hardening/vsftpd

02 - SQL Injection

Se ha detectado un campo vulnerable a la explotación de SQL Injection. Este campo se encuentra en la URL http://192.168.50.251/dvwa/vulnerabilities/sqli/ y es el campo de User ID. Tras realizar una exploración básica introduciendo una simple comilla (‘) el servicio nos muestra un error de sintaxis dándonos a entender que es vulnerable a explotaciones debido a la no sanitización del input del usuario. Utilizando payloads más sofisticados, hemos podido comprobar que se tiene acceso a toda la base de datos del servicio.

Prueba de concepto :



Recomendación :

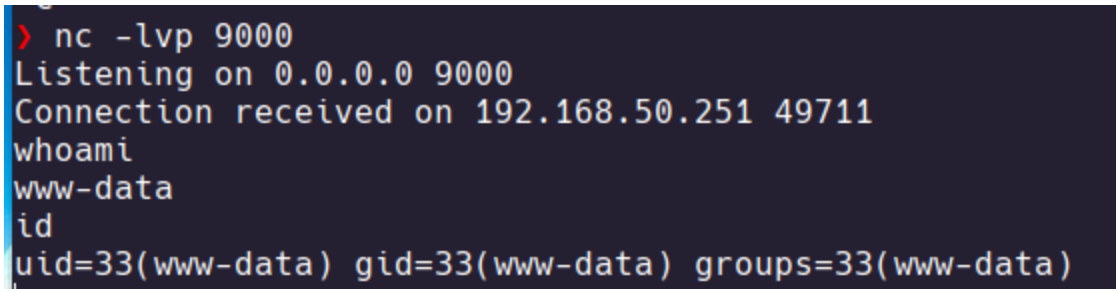
- Sanitización del input del usuario y aplicar validación por whitelist aceptando sólo lo que se espera
- Usando el menor privilegio posible para la cuenta de la aplicación

Referencia :

https://owasp.org/www-community/attacks/SQL_Injection

03 - Upload File Inclusion

Dentro del activo se ha encontrado un campo en el que podemos seleccionar un archivo cuya extensión no es comprobada antes de su subida al servidor, dando lugar a la subida de archivos maliciosos y dando pie a su ejecución desde el lado del servidor.
Este campo se encuentra en la URL http://192.168.50.251/dvwa/vulnerabilities/upload/ del activo metasploitable2.
Prueba de concepto : Se ha elaborado un archivo PHP encargado de ejecutar código en el sistema.Para ejecutar código, primero vamos al nuevo recurso subido a la web y en el parámetro configurado introducimos el código que creará una conexión a nuestra dirección IP y nos permitirá ejecutar una shell con el usuario www-data poniéndonos a la escucha.



Recomendación :

- Validar por whitelist lo que se permite subir al servidor y comprobar los magic-bytes para hacer validación
- Renombrar archivos y control de rutas para así evitar que el usuario controle estos parámetros.
- Limitar el tamaño de los archivos

Referencia :

https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
https://www.securitum.com/unrestricted_file_upload_leading_to_arbitrary_code_execution.html

04 - Bind Shell

Este servicio es crítico ya que existe expuesto un puerto en el cual existe una shell como usuario root y su acceso es simple y directo.
Esto se debe a un compromiso previo del sistema o instalación de un backdoor.

Prueba de concepto :

```
❯ nc 192.168.50.251 1524
root@metasploitable:/# whoami
root
root@metasploitable:/#
```

Recomendación :

- Cerrar de inmediato el puerto
- Reinstalar o restaurar el sistema operativo desde una copia de seguridad limpia

05 - PostgreSQL Code Execution

Se ha encontrado que en el puerto 5432 existe una versión la cual tiene diferentes vulnerabilidades expuestas. Concretamente, la versión que se usa en el activo contiene un exploit ejecutable desde el framework metasploit junto con un payload para postgres. Aquí hemos seleccionado el objetivo, en este caso es la IP 192.168.50.251 y puesto nuestra dirección IP para obtener una shell y ejecutamos. Esto nos da una shell con el usuario que lo ejecuta que en este caso es postgres.

Prueba de concepto :

```
postgres@metasploitable:~$ whoami
postgres
postgres@metasploitable:~$
```

Recomendación :

- Migrar a una versión más moderna que tenga soporte
- Configurar una autenticación más robusta ya que es nula
- Restringir el uso a usuarios internos o con VPN

Referencias :

https://bernardodamele.blogspot.com/2009/01/command-execution-with-postgresql-udf.html

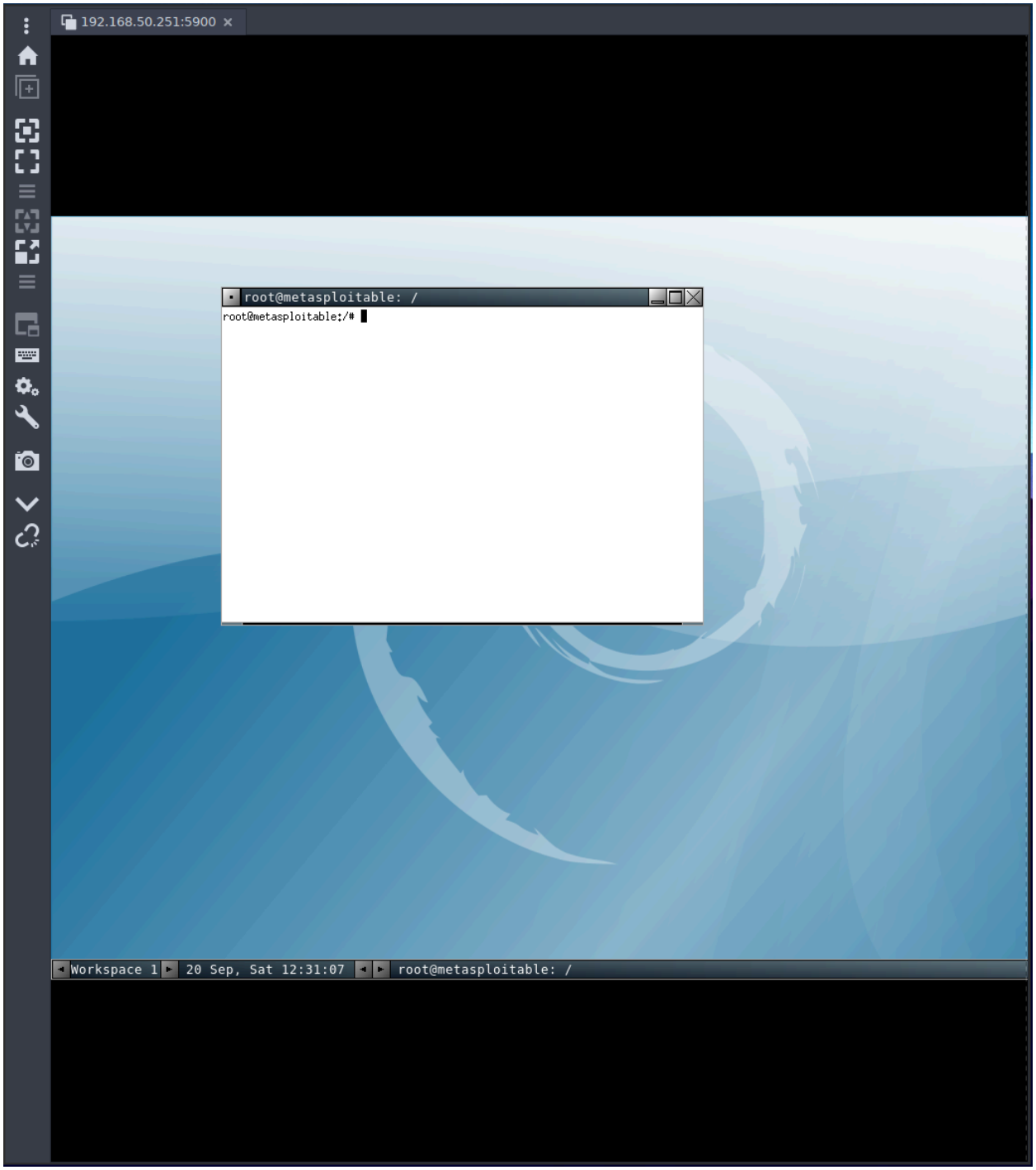
https://www.cybertec-postgresql.com/en/postgresql-security-things-to-avoid-in-real-life/

06 - VNC Login

Se ha detectado que el puerto 5900 se encuentra abierto corriendo el servicio VNC protocol 3.3 sin ninguna seguridad ya que es un protocolo sin cifrar, contraseñas débiles y fácil de interceptar. Para la explotación de este servicio se ha encontrado un módulo en metasploit el cual logra dándole un usuario legítimo, obtener la contraseña para el login y prueba a hacer login con una de esas contraseñas. En este caso, al carecer de credenciales, utilizamos uno de los usuarios que hemos podido obtener a través de la explotación del servicio SMB y obtenemos que podemos hacer login con el usuario *root* y password *password.*

Prueba de concepto :

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> run
[*] 192.168.50.251:5900    - 192.168.50.251:5900 - Starting VNC login sweep
[!] 192.168.50.251:5900    - No active DB -- Credential data will not be saved!
[+] 192.168.50.251:5900    - 192.168.50.251:5900 - Login Successful: :password
[*] 192.168.50.251:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> exit
```



Recomendación :

- Actualizar la versión de VNC a una más moderna con soporte de cifrado

- Encapsular VNC dentro de una VPN o usar alternativas seguras como RDP con TSL
- Forzar el uso de contraseñas fuertes y deshabilitar el login anónimo

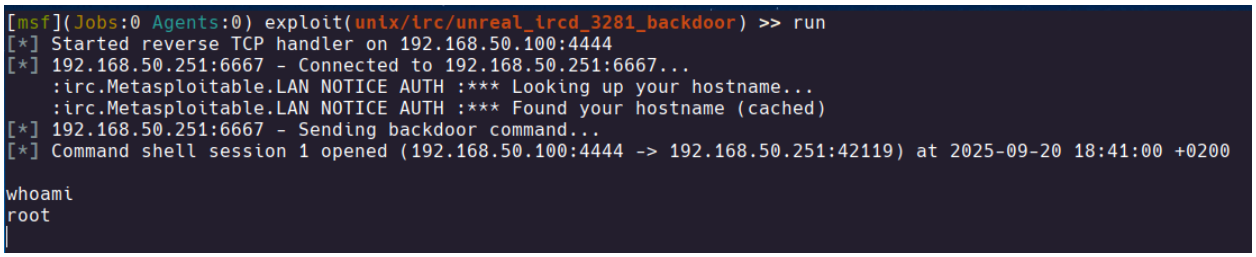
Referencia :

https://security.stackexchange.com/questions/124958/how-do-i-assess-and-mitigate-the-security-risks-of-a-vnc-tool

07 - IRC Backdoor

Se ha detectado que en el activo se está exponiendo el puerto 6667 el cual tiene un servicio de UnrealIRC. Este servicio tiene vulnerabilidades debido a que su instalación ha podido ser desde una distribución comprometida y esta tiene un backdoor el cual nos da acceso remoto al sistema. Este backdoor es fácilmente ejecutable mediante el framework metasploit *unreal_ircd_3281_backdoor*. Una vez configurado todos los parámetros necesarios, ejecutamos y obtenemos una shell como root.

Prueba de concepto :



Recomendación :

- Desinstalar IRC e instalarlo desde una fuente segura
- Monitorizar las conexiones salientes que puedan ser sospechosas

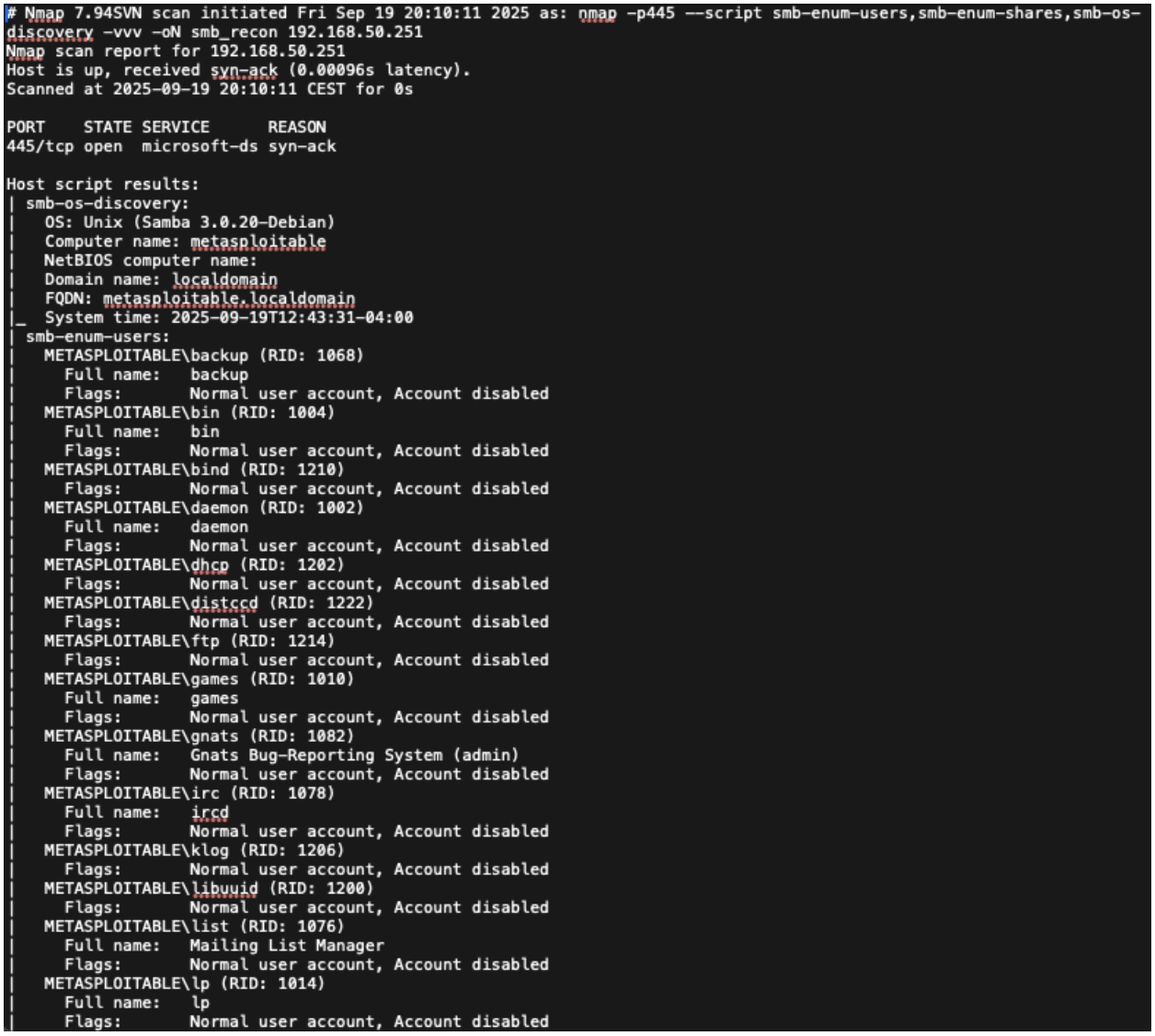
Referencia :

https://nmap.org/nsedoc/scripts/irc-unrealircd-backdoor.html

08 - SMB Enumeration

Se ha detectado que el activo tiene expuesto el puerto 445 con el servicio de smb el cual tiene múltiples vulnerabilidades si no está correctamente configurado. Con el mismo nmap, se ha podido enumerar usuarios del sistema, carpetas compartidas y el sistema operativo del activo sin necesidad de credenciales. Con esta información podemos hacer un mapa de la superficie a atacar.

Prueba de concepto :



```
# Nmap 7.94SVN scan initiated Fri Sep 19 20:10:11 2025 as: nmap -p445 --script smb-enum-users,smb-enum-shares,smb-os-discovery -vvv -oN smb_recon 192.168.50.251
Nmap scan report for 192.168.50.251
Host is up, received syn-ack (0.00096s latency).
Scanned at 2025-09-19 20:10:11 CEST for 0s

PORT    STATE SERVICE      REASON
445/tcp open  microsoft-ds syn-ack

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-09-19T12:43:31-04:00
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name:   Gnats Bug-Reporting System (admin)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\irc (RID: 1078)
|     Full name:   ircd
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\klog (RID: 1206)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\libuuid (RID: 1200)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\list (RID: 1076)
|     Full name:   Mailing List Manager
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\lp (RID: 1014)
|     Full name:   lp
|     Flags:       Normal user account, Account disabled
```

```
|   METASPLOITABLE\mail (RID: 1016)
|     Full name:   mail
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\man (RID: 1012)
|     Full name:   man
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\msfadmin (RID: 3000)
|     Full name:   msfadmin,,,
|     Flags:       Normal user account
|   METASPLOITABLE\mysql (RID: 1218)
|     Full name:   MySQL Server,,,
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\news (RID: 1018)
|     Full name:   news
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\nobody (RID: 501)
|     Full name:   nobody
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\postfix (RID: 1212)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\postgres (RID: 1216)
|     Full name:   PostgreSQL administrator,,,
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\proftpd (RID: 1226)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\proxy (RID: 1026)
|     Full name:   proxy
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\root (RID: 1000)
|     Full name:   root
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\service (RID: 3004)
|     Full name:   ,,,
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\sshd (RID: 1208)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\sync (RID: 1008)
|     Full name:   sync
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\sys (RID: 1006)
|     Full name:   sys
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\syslog (RID: 1204)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\telnetd (RID: 1224)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\tomcat55 (RID: 1220)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\user (RID: 3002)
|     Full name:   just a user,111,,
|     Flags:       Normal user account
|   METASPLOITABLE\uucp (RID: 1020)
|     Full name:   uucp
|     Flags:       Normal user account, Account disabled
```

```
|   METASPLOITABLE\telnetd (RID: 1224)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\tomcat55 (RID: 1220)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\user (RID: 3002)
|     Full name:   just a user,111,,
|     Flags:       Normal user account
|   METASPLOITABLE\uucp (RID: 1020)
|     Full name:   uucp
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\www-data (RID: 1066)
|     Full name:   www-data
|_    Flags:       Normal user account, Account disabled
| smb-enum-shares:
|   account_used: <blank>
|   \\192.168.50.251\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.50.251\IPC$:
|     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
|   \\192.168.50.251\opt:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.50.251\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|   \\192.168.50.251\tmp:
|     Type: STYPE_DISKTREE
|     Comment: oh noes!
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|_    Anonymous access: READ/WRITE

Read data files from: /usr/bin/../share/nmap
# Nmap done at Fri Sep 19 20:10:11 2025 -- 1 IP address (1 host up) scanned in 0.41 seconds
```

Recomendación :

- No exponer SMB a internet y permitir únicamente el acceso desde redes internas
- Bloquear SMBv1 y forzar SMB2/SMB3 con cifrado
- Mejorar los permisos en las carpetas compartidas

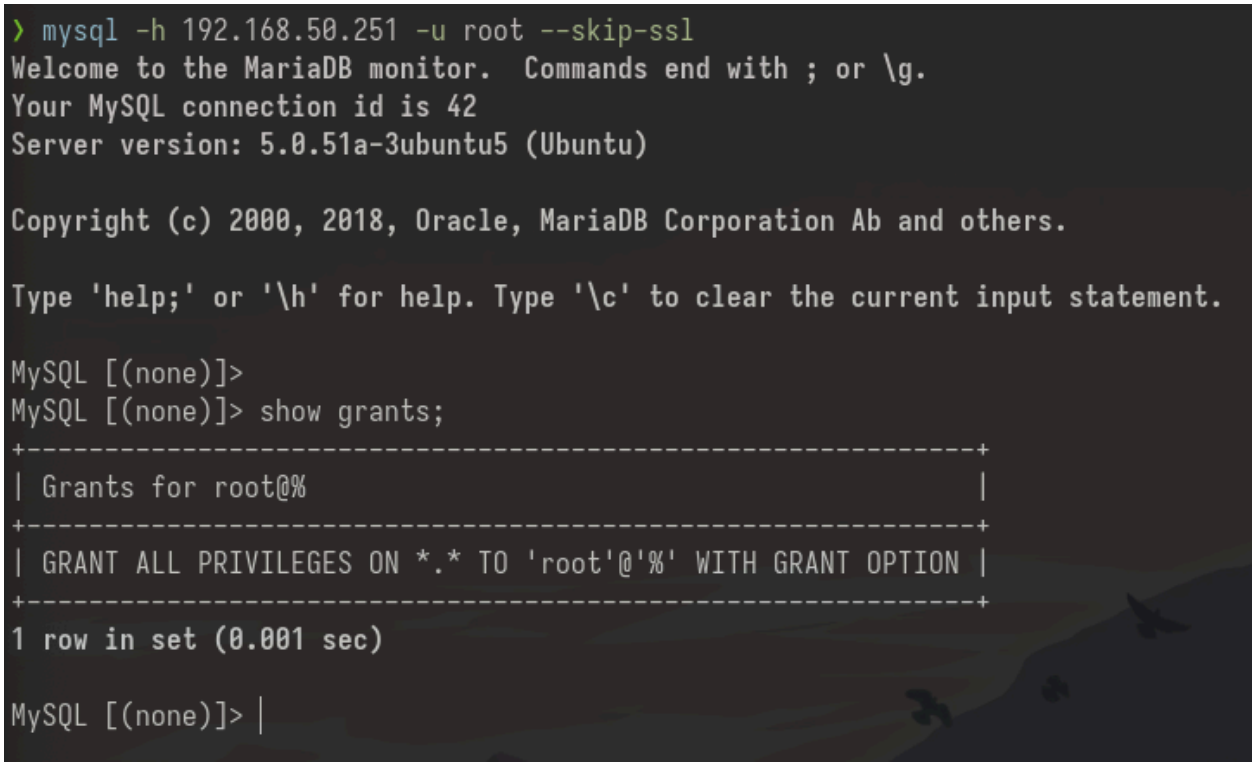
Referencia :

https://hackviser.com/tactics/hardening/smb

09 - MySQL Insecure Login

Se ha detectado que el puerto 3306 está expuesto y corre un servicio MySQL 5.0.51 el cual carece de contraseñas y da permiso sin credenciales a la base de datos como usuario root el cual tiene todos los privilegios posibles. Esto permite que se puedan robar, eliminar o alterar datos, tablas o bases de datos teniendo un riesgo muy crítico para la empresa.

Prueba de concepto :



Recomendación:

- Securizar el usuario root y eliminar cuentas que no estén en uso
- Dar a los usuarios los mínimos privilegios
- Restringir el acceso a redes internas
- Forzar cifrado

Referencia :

https://cloud.google.com/mysql/hardening-mysql?hl=en

https://www.bytebase.com/reference/mysql/how-to/mysql-security-best-practices/