ELYSIUM

NSATTECH SOLUTIONS

Informe de Evaluación de Exposición y Vulnerabilidades

Pentester : Daniel Arconada

Índice

Acuerdo de Confidencialidad

Elysium y NSATTECH acuerdan llevar a cabo una actividad de pruebas de penetración sobre el activo identificado con la dirección IP 192.168.50.251.
El propósito de esta actividad es evaluar la postura de seguridad del sistema e identificar posibles vulnerabilidades que puedan afectar a la organización, durante el período del 19 al 24 de septiembre de 2025.
Ambas partes acuerdan que toda la información obtenida durante el proceso será tratada bajo estricta confidencialidad.
Ningún dato, hallazgo o resultado será compartido con terceros ajenos a las empresas mencionadas.
Los resultados del análisis se utilizarán exclusivamente para mejorar la seguridad de NSATTECH y no se divulgarán fuera del alcance de esta colaboración con Elysium.

Información de Contacto

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

Introducción

Se llevó a cabo una evaluación de pruebas de penetración sobre el activo designado por NSATTECH con el objetivo de evaluar su exposición frente a posibles amenazas.

El objetivo principal de esta actividad fue mejorar la postura de seguridad de la organización y mitigar riesgos operativos que pudieran derivarse de un incidente de seguridad.
Durante la evaluación se identificaron varias vulnerabilidades y debilidades potenciales que, en condiciones reales, podrían ser explotadas para comprometer la confidencialidad de los datos, obtener accesos no autorizados, interrumpir la disponibilidad de servicios o ejecutar código malicioso dentro del entorno.
Este informe resume los hallazgos identificados junto con un conjunto de recomendaciones y acciones de remediación destinadas a mejorar la seguridad de los activos de NSATTECH y reforzar su capacidad de defensa frente a amenazas externas.

Alcance

Para esta actividad de pruebas de penetración, **NSATTECH** ha seleccionado el siguiente activo objetivo para su evaluación:

Host	Dirección IP
metasploitable2	192.168.50.251

Escenarios Fuera de Alcance

El alcance de esta evaluación excluye explícitamente cualquier prueba de denegación de servicio (DoS/DDoS), así como técnicas de ingeniería social como phishing, vishing, smishing o suplantación de identidad.

Estas restricciones aseguran que la evaluación se limite al activo autorizado, evitando cualquier impacto potencial sobre la operativa del negocio, el personal o terceros no involucrados.

Clasificación de Riesgo

La siguiente tabla presenta los criterios de clasificación de riesgo utilizados para categorizar las vulnerabilidades identificadas según su severidad y potencial impacto.

Criticidad	Rango CVSS	Descripción
Alta	8.1-10.0	Indica un riesgo crítico que es fácilmente explotable. Se recomienda remediación inmediata tras su descubrimiento.
Media	6.1-8.0	Representa una vulnerabilidad significativa que puede ser explotada bajo ciertas condiciones. Debe abordarse tan pronto como se resuelvan las de alta severidad.
Baja	4.1-6.0	Identifica una debilidad moderada que puede ser difícil de explotar. Se recomienda su corrección dentro de los 90 días posteriores a su detección.

Resumen Ejecutivo

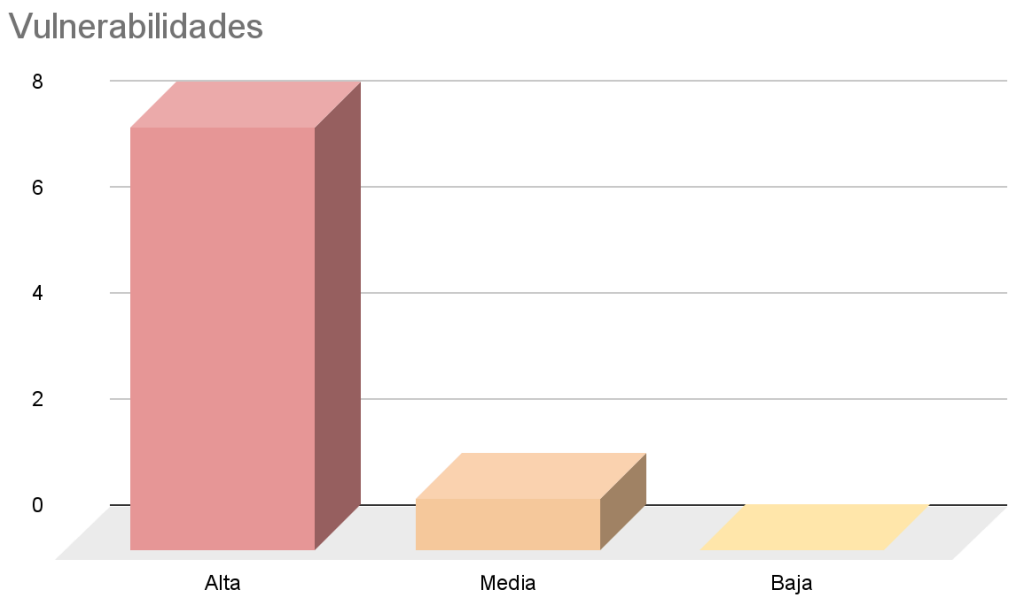
La evaluación de seguridad realizada sobre el activo objetivo ha revelado que NSATTECH se encuentra actualmente expuesta a varios riesgos que podrían tener un impacto severo en sus operaciones y reputación corporativa.

Si estas vulnerabilidades no se abordan, podrían provocar pérdida o alteración de información crítica, interrupción de servicios o un impacto directo en clientes y socios. Estos eventos podrían generar costes inesperados de recuperación, sobrecarga en la gestión de incidentes, implicaciones regulatorias y una pérdida significativa de confianza por parte de los interesados.

En términos prácticos, no mitigar estos riesgos ahora aumenta la probabilidad de que un futuro incidente escale hasta una crisis a gran escala, afectando tanto al rendimiento financiero como a la credibilidad de la organización.

Tomar medidas inmediatas de remediación es, por tanto, esencial para proteger los activos clave, asegurar la continuidad operativa y mantener la confianza de clientes, socios y partes interesadas.

Clasificación de Vulnerabilidades



Resumen de Vulnerabilidades

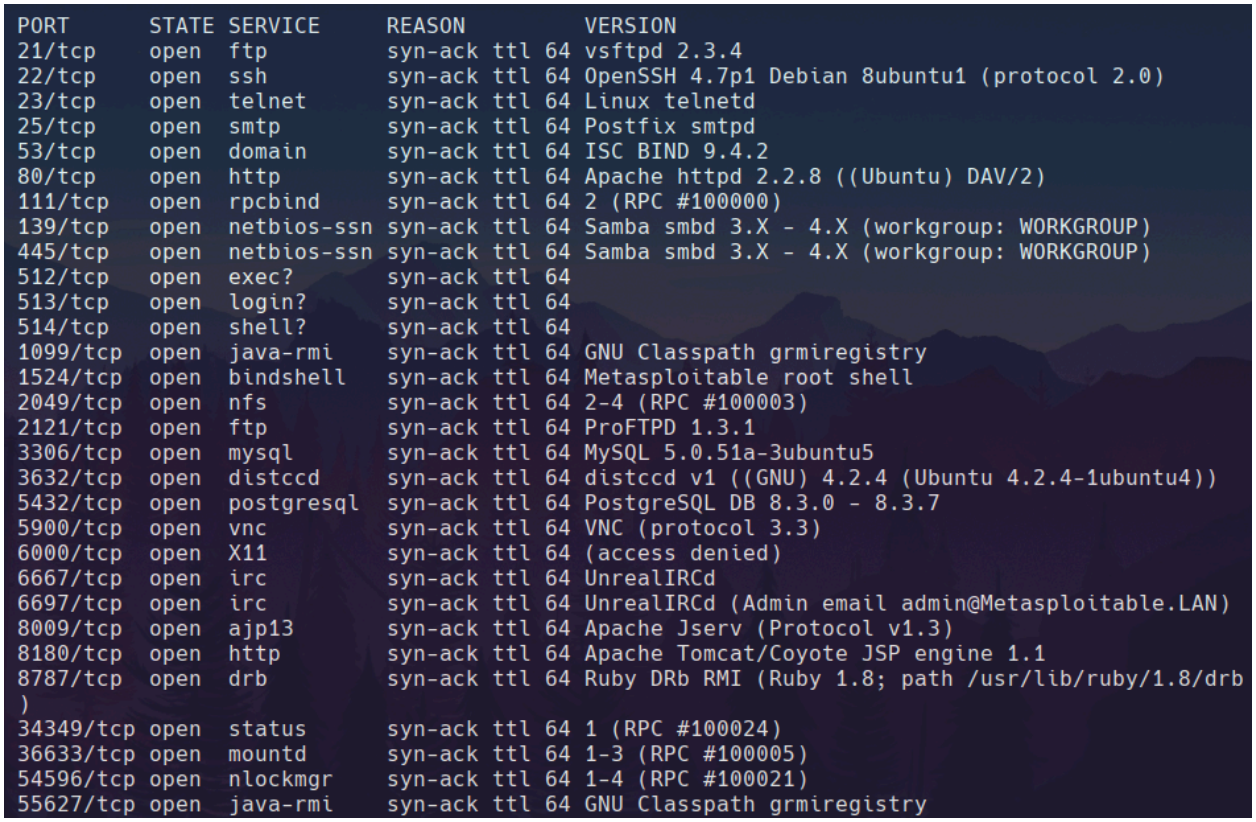
ID Vulnerabilidad - Nombre	Recomendación	Impacto	Clasificación CVSS
01 - Backdoor FTP	Actualizar a una versión segura y mantenida de vsftpd para eliminar vulnerabilidades conocidas de backdoor.	Alta	10
02 - Inyección SQL	Implementar validación estricta del input y consultas parametrizadas para evitar la ejecución arbitraria de comandos SQL.	Alta	9.5
03 - File Inclusion	Aplicar una política de lista blanca para tipos de archivo permitidos y validar extensiones tanto del lado cliente como servidor.	Alta	9.7
04 - Bind Shell	Cerrar el puerto afectado y eliminar cualquier proceso no autorizado de bind shell para prevenir acceso remoto.	Alta	10
05 - Ejecución de código en PostgreSQL	Actualizar PostgreSQL a la versión estable más reciente para mitigar vulnerabilidades conocidas de ejecución de código.	Alta	9.0
06 - Acceso inseguro a VNC	Aplicar políticas de contraseñas fuertes y actualizar el servicio VNC a la versión más segura disponible.	Alta	9.3
07 - Backdoor IRC	Deshabilitar o actualizar el servicio IRC para eliminar el backdoor y prevenir canales de comunicación no autorizados.	Alta	9.8

08 - Enumeración de SMB	Restringir el acceso SMB a redes de confianza y deshabilitar sesiones anónimas para limitar la exposición de información.	Media	7.8
09 - Inicio de sesión inseguro en MySQL	Implementar autenticación robusta, restringir acceso remoto y aplicar buenas prácticas de configuración segura.	Alta	9.8

Análisis Técnico

La siguiente captura se usa como referencia y muestra los puertos descubiertos y explotados mediante un escaneo de red con nmap sobre el activo objetivo.

nmap -sS -sV -p- -n -Pn -v 192.168.50.251



```
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
```

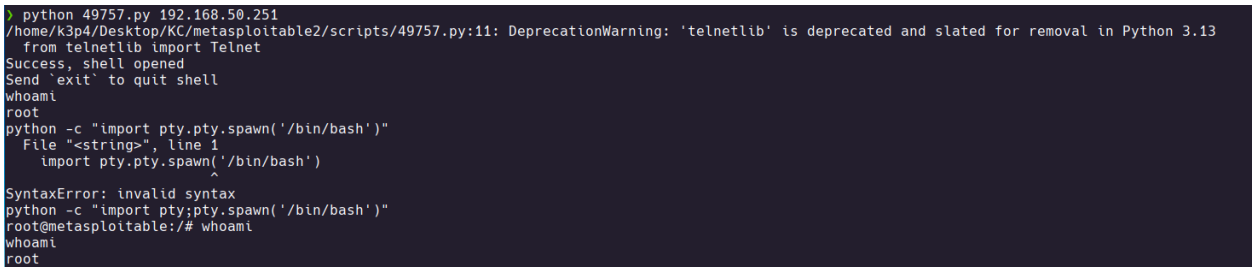
01 - Ejecución de Comandos mediante Backdoor FTP

Se identificó un servicio FTP vulnerable en el puerto 21, ejecutando vsftpd 2.3.4, el cual está asociado al CVE-2011-2523.

Esta vulnerabilidad provoca la instalación de un backdoor remoto que escucha en el puerto 6200.

Bajo condiciones que explotan este CVE, un atacante puede activar el backdoor y obtener una shell remota con privilegios elevados.

Prueba de concepto:



Recomendaciones para NSATTECH:

- Actualizar o aplicar parches al servicio FTP a una versión segura y con soporte. Si no existe una versión actualizada, discontinuar el uso de la instancia afectada de vsftpd.
- Restringir el acceso al servicio FTP en el perímetro de red (firewall/ACL) para que solo las IP autorizadas puedan alcanzar el puerto 21.
- Sustituir el servicio FTP por una alternativa más segura (SFTP/FTPS o una solución gestionada de transferencia segura de archivos).
- Fortalecer y monitorear: aplicar autenticación robusta, habilitar registros/alertas para actividad anómala de FTP y realizar comprobaciones de integridad periódicas sobre archivos críticos del sistema.

Referencias:

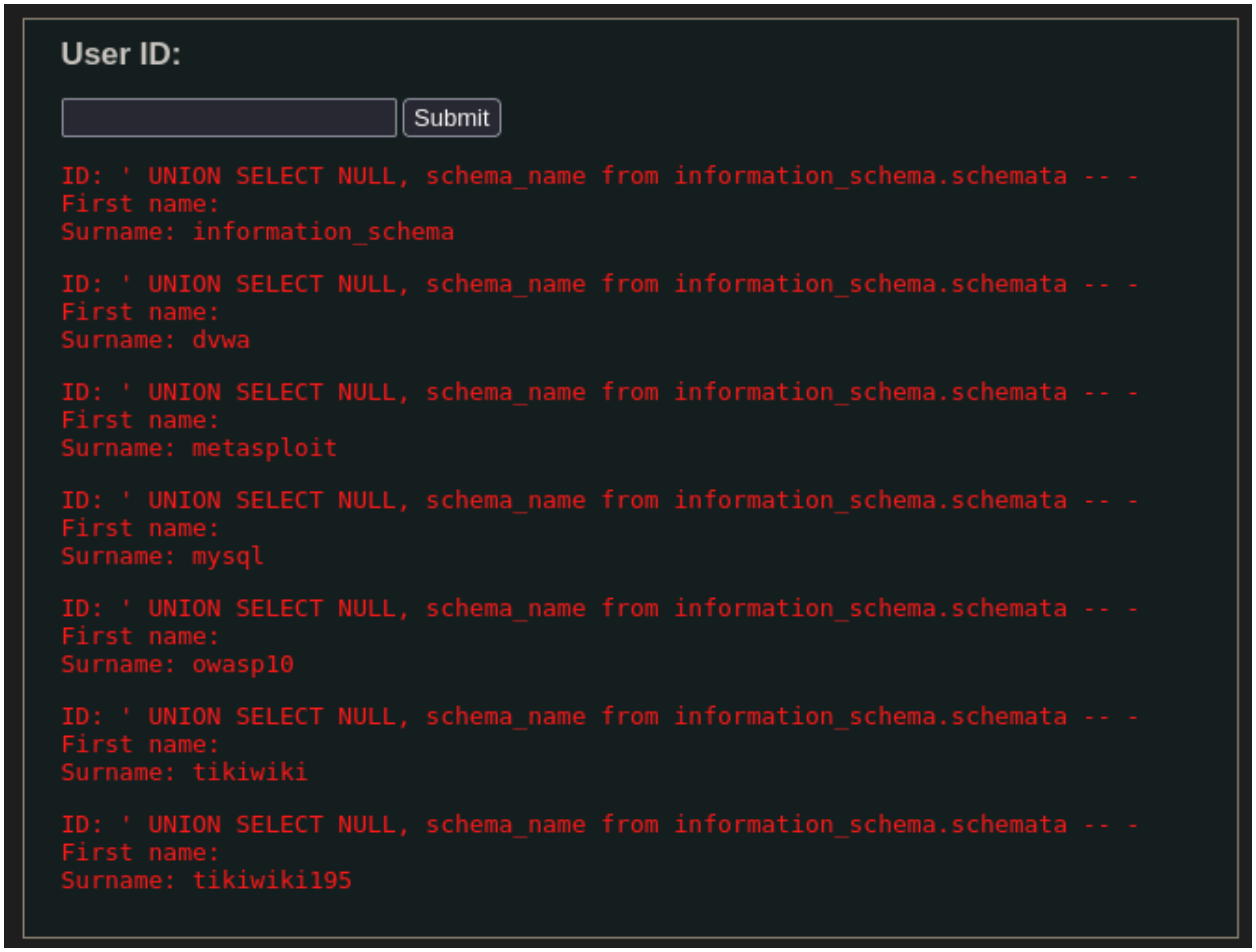
https://hackviser.com/tactics/hardening/vsftpd

02 - Inyección SQL

Se identificó una vulnerabilidad de inyección SQL en el parámetro User ID en http://192.168.50.251/dvwa/vulnerabilities/sqli/.
Una prueba básica con una comilla simple (') produjo un error de sintaxis de base de datos, lo que indica falta de validación del input y manejo inadecuado de errores.
Pruebas adicionales confirmaron que la vulnerabilidad permite extraer todo el contenido

de la base de datos del servicio.

Prueba de concepto:



Recomendaciones para NSATTECH:

- Aplicar sanitización estricta de la entrada del usuario e implementar una política de validación basada en lista blanca, aceptando únicamente los valores esperados (longitud de entrada, caracteres permitidos, tipos MIME y extensiones de archivo).
- Combinar con codificación de salida contextual y manejo adecuado de errores para evitar rastros de pila o mensajes informativos de base de datos.
- Operar la aplicación bajo el principio de privilegio mínimo: la cuenta de la aplicación debe tener únicamente los permisos necesarios, sin privilegios de

superusuario/administrador, y separar las cuentas de administración, aplicación y mantenimiento.

Referencias:

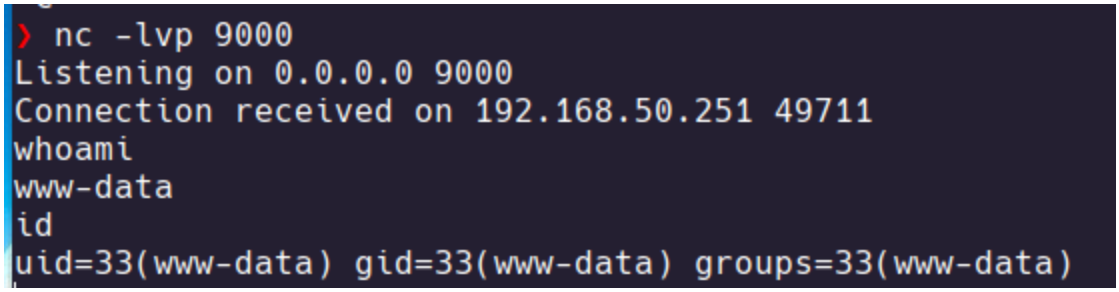
https://owasp.org/www-community/attacks/SQL_Injection

03 - File Inclusion

Se identificó una vulnerabilidad de file inclusion disponible en http://192.168.50.251/dvwa/vulnerabilities/upload/ dentro del activo Metasploitable2. La aplicación no valida la extensión del archivo ni realiza comprobaciones suficientes en el servidor antes de almacenarlo, lo que permite a un atacante subir un script malicioso y ejecutarlo en el servidor.

Prueba de concepto:

Se creó un archivo PHP capaz de ejecutar código arbitrario en el sistema. Al acceder al recurso subido y proporcionar el parámetro configurado con el payload, el script establece una conexión con la IP del atacante y provee una shell remota como usuario www-data.



Recomendaciones para NSATTECH:

- Aplicar validación en el servidor basada en lista blanca de tipos de archivo permitidos y verificar el contenido usando magic bytes / detección de tipo MIME, además de la extensión.
- Implementar manejo de archivos y control de rutas seguro: sanitizar y

reemplazar los nombres de archivo proporcionados por el usuario con nombres aleatorios generados; almacenar los archivos fuera del directorio raíz del servidor web para evitar inyecciones de ruta o nombre.

- Imponer límites estrictos al tamaño de los archivos a nivel de servidor (validar Content-Length o flujo), configurar el servidor para rechazar cargas grandes y aplicar límites de recursos para prevenir agotamiento.

Referencias:

https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

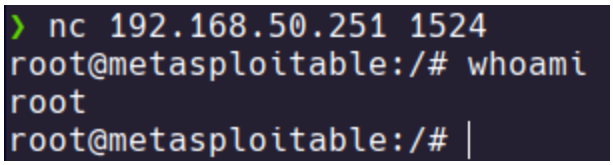
https://www.securitum.com/unrestricted_file_upload_leading_to_arbitrary_code_execution.html

04 - Bind Shell

El servicio se clasifica como crítico porque el host expone un puerto de red que proporciona una shell como root sin autenticación.

Esta condición es indicativa de un compromiso previo del sistema o de la presencia de un backdoor persistente en el activo.

Prueba de concepto:

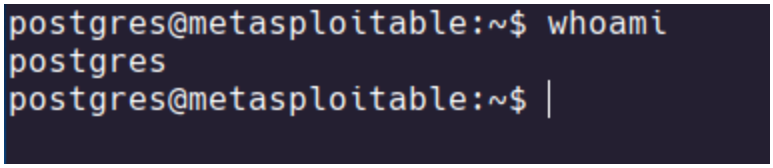


Recomendaciones para NSATTECH:

- Cerrar de inmediato el puerto afectado tanto en el perímetro de red como en el host para evitar más accesos no autorizados.
- Reinstalar o restaurar el host desde una imagen verificada o copia de seguridad limpia: aislar el sistema, realizar una captura forense y aplicar todos los parches de seguridad y configuraciones reforzadas antes de volverlo a conectar a la red.

05 - Ejecución de Código en PostgreSQL

Se detectó una instancia vulnerable de PostgreSQL en el puerto 5432.
La versión que se ejecuta en el activo contiene múltiples vulnerabilidades explotables y es susceptible a exploits públicos conocidos.
Pruebas controladas confirmaron que un exploit dirigido a esta versión puede resultar en ejecución remota de código, obteniendo una shell remota con privilegios del usuario postgres.
Prueba de concepto:



Recomendaciones para NSATTECH:

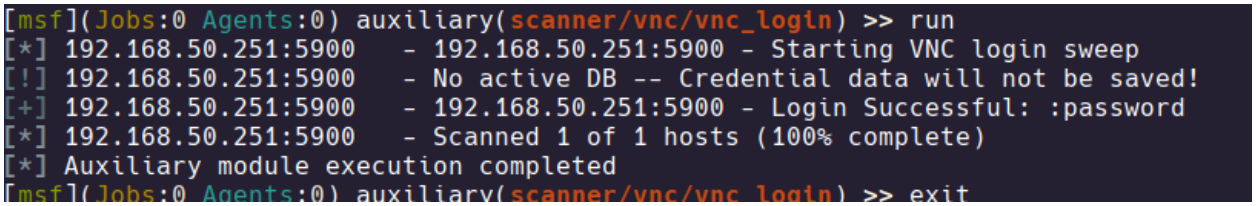
- Migrar a una versión moderna con soporte. Actualizar la base de datos a una versión actualmente soportada y establecer un proceso de gestión de parches para aplicar actualizaciones de seguridad con rapidez.
- Configurar autenticación robusta. Sustituir la autenticación actual por mecanismos más seguros, aplicar políticas de contraseñas fuertes, usar métodos de autenticación seguros y considerar MFA para accesos administrativos.
- Restringir la exposición de red únicamente a usuarios de confianza. Limitar el acceso a subredes internas o redes de gestión; requerir acceso por VPN o bastión para administración remota.

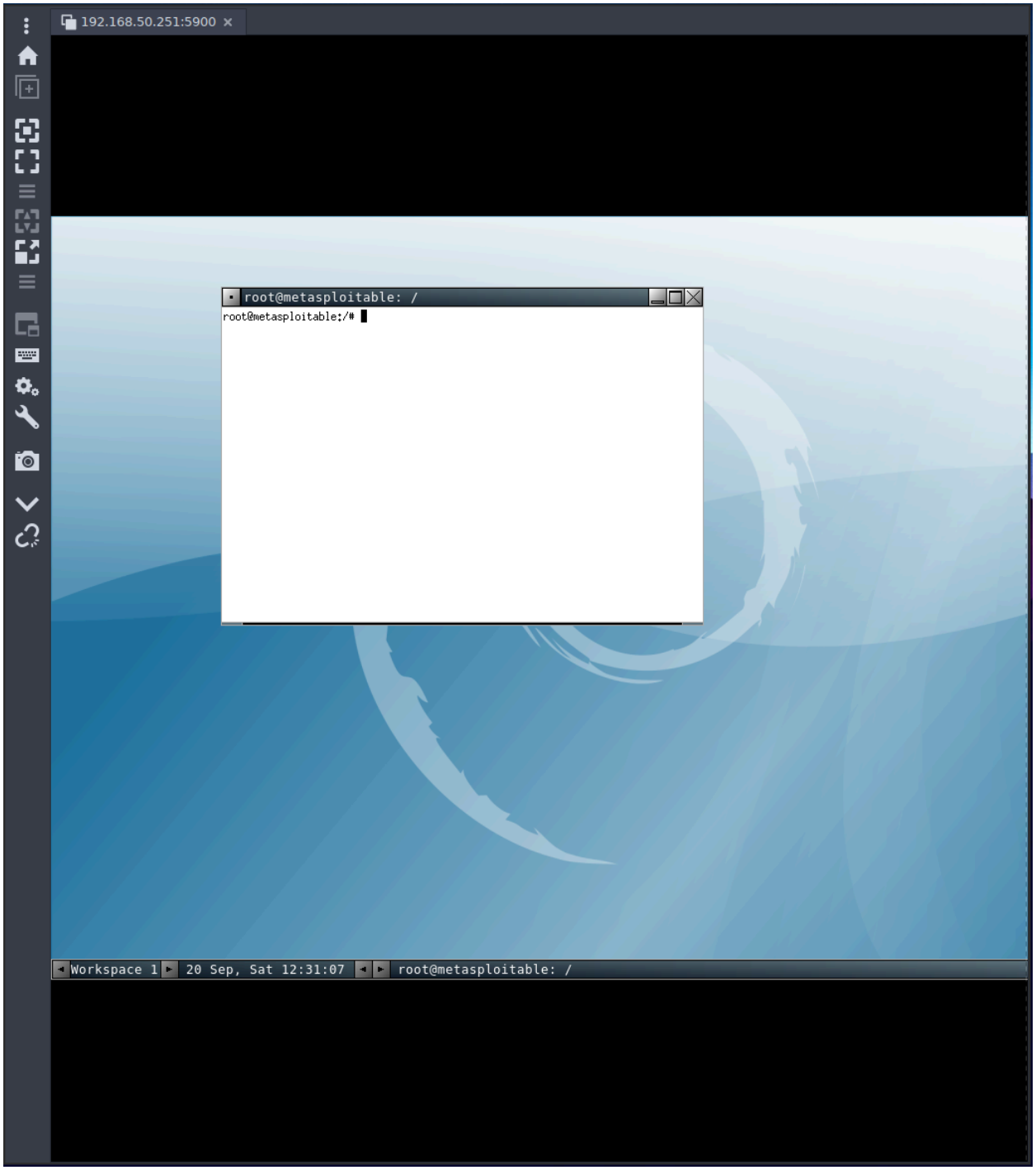
Referencias:
https://bernardodamele.blogspot.com/2009/01/command-execution-with-postgresql-udf.html

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

06 - Login en VNC

Se identificó un servicio VNC no seguro en el puerto 5900.
El servicio transmite datos sin cifrar, es susceptible de ser interceptado y está protegido con una autenticación débil.
Durante las pruebas se identificó un módulo en Metasploit capaz de obtener credenciales válidas con un nombre de usuario legítimo.
Usando credenciales obtenidas previamente desde el servicio SMB comprometido, se logró autenticar exitosamente: root / password permitió el acceso VNC.
Prueba de concepto:





Recomendaciones para NSATTECH:

- Actualizar VNC a una versión moderna con soporte y cifrado incorporado.
- Encapsular el tráfico VNC dentro de una VPN o usar alternativas seguras como

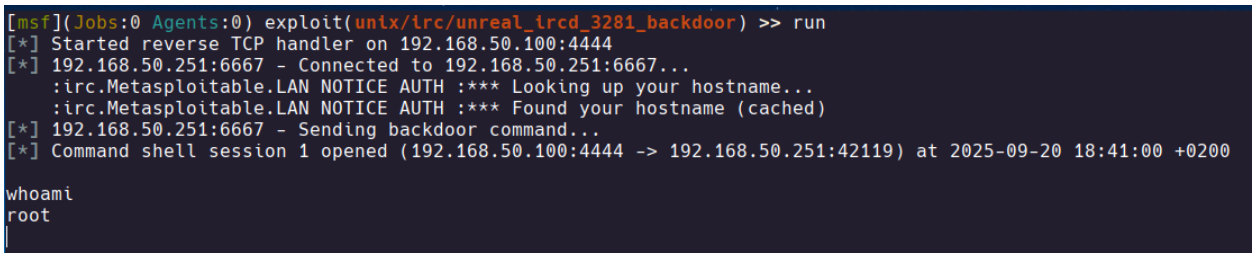
RDP sobre TLS.

- Forzar políticas de contraseñas fuertes y deshabilitar logins anónimos o no autenticados, aplicando bloqueo de cuenta y monitoreo de intentos anómalos.

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

07 - Backdoor IRC

Se detectó un servicio UnrealIRCd escuchando en el puerto 6667.
La instalación parece provenir de una distribución potencialmente comprometida que incluye un backdoor que permite el acceso remoto al host.
Este backdoor está asociado al módulo de Metasploit unreal_ircd_3281_backdoor.
La explotación exitosa de esta vulnerabilidad puede resultar en ejecución remota de código y en la obtención de una shell como usuario root en el sistema afectado.
Prueba de concepto:



Recomendaciones para NSATTECH:

- Desinstalar el servicio IRC e instalarlo desde una fuente segura y verificada. Asegurarse de que los paquetes de instalación provengan de repositorios oficiales o versiones comprobadas mediante checksum, verificando su integridad antes de desplegar.
- Monitorizar y alertar sobre conexiones salientes sospechosas. Implementar monitorización de red para detectar tráfico anómalo de salida, establecer una

línea base de comportamiento y generar alertas ante destinos poco comunes, conexiones persistentes o iniciadas por procesos no esperados.

Referencias:

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

08 - Enumeración de SMB

Se identificó un servicio SMB en el puerto 445.

Si está mal configurado, SMB puede exponer múltiples vulnerabilidades.

Utilizando el mismo escaneo con nmap, fue posible enumerar usuarios del sistema, directorios compartidos y el sistema operativo del host objetivo sin necesidad de autenticación.

Esta información permite construir un mapa de la superficie de ataque, facilitando posteriores fases de explotación o movimientos laterales.

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
```

Recomendaciones para NSATTECH:

- No exponer SMB a Internet; permitir acceso únicamente desde redes internas o de confianza.
- Deshabilitar SMBv1 y forzar el uso de SMB2/SMB3 con cifrado. Asegurar que los protocolos antiguos sean eliminados y que los dialectos modernos estén configurados con firma y cifrado habilitados.
- Reforzar los permisos de las carpetas compartidas. Aplicar el principio de mínimo privilegio, eliminar accesos anónimos o de invitado y reducir la

pertenencia a grupos con acceso compartido.

Referencias:

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

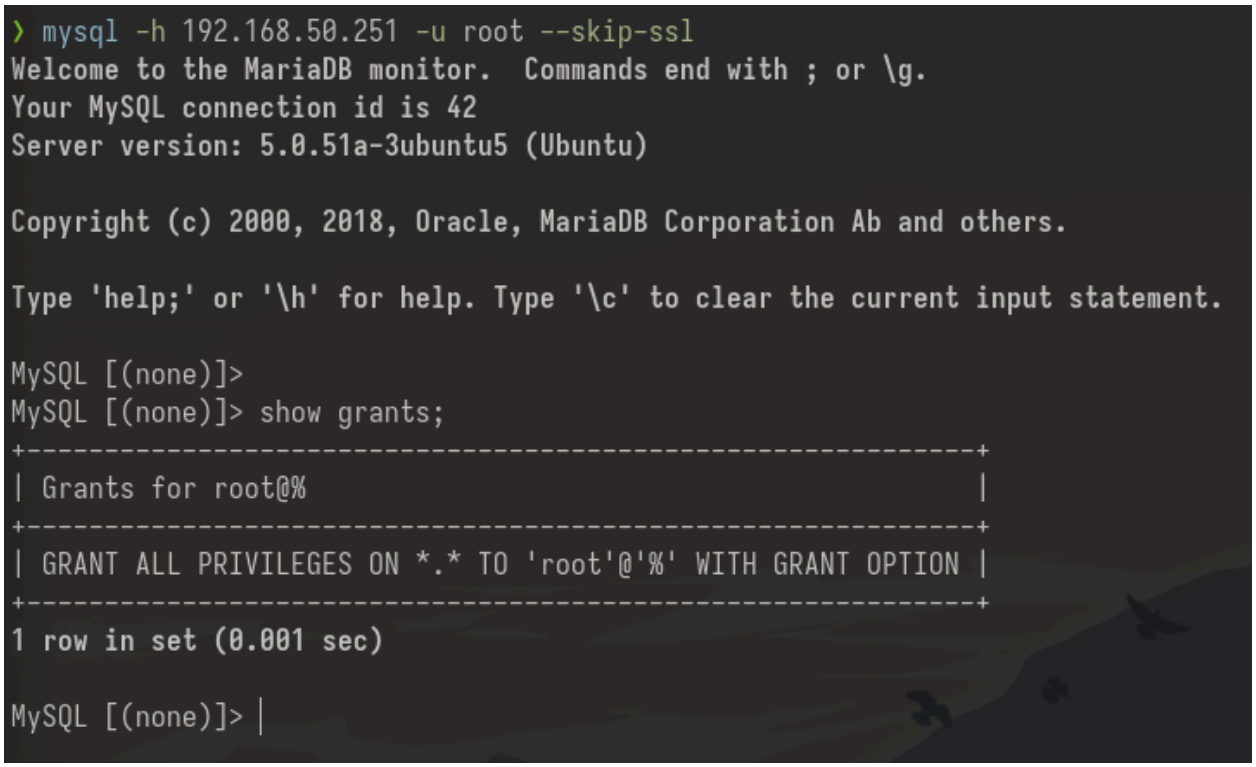
09 - Inicio de Sesión Inseguro en MySQL

Se encontró un servicio MySQL 5.0.51 expuesto en el puerto 3306.

El servicio permite acceso sin autenticación al usuario root, otorgando privilegios administrativos completos a cualquier conexión remota.

Esta mala configuración permite a un atacante leer, modificar o eliminar datos, tablas e incluso bases de datos completas, representando un riesgo crítico para la organización.

Prueba de concepto:



Recomendaciones para NSATTECH:

- Asegurar la cuenta root y eliminar cuentas predeterminadas o no utilizadas.

Aplicar autenticación fuerte y garantizar que el usuario root sólo sea accesible de manera local.

- Aplicar el principio de privilegio mínimo: asignar a los usuarios únicamente los permisos estrictamente necesarios para sus tareas operativas.
- Restringir el acceso a redes internas o de confianza, bloqueando conexiones remotas desde orígenes externos o no autorizados.
- Forzar el uso de conexiones cifradas entre los clientes y el servidor MySQL (por ejemplo, SSL/TLS) para proteger las credenciales y los datos en tránsito.

Referencias:

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

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