INFORME TÉCNICO DE AUDITORÍA DE SEGURIDAD

Pentesting de Servicio FTP (Caja Gris)
Servidor Crítico - Hospital General de Madrid (ficticio)

Activo Objetivo: Servidor Linux (192.168.122.10)

Vulnerabilidad Principal: Acceso Anónimo (ftp-anon)

Auditor: Arturo Martín-Vegue

Fecha de Emisión: 6 de Enero de 2026

Índice

1. Resumen Ejecutivo

Como parte de la evaluación continua de seguridad del Hospital General de Madrid, se ha realizado una auditoria de caja gris sobre el servidor crítico `192.168.122.10`, con el objetivo de identificar vulnerabilidades que pudieran comprometer la confidencialidad de los datos.

Durante el análisis, se detectó una **vulnerabilidad de severidad MEDIA** en el servicio de transferencia de archivos (FTP). Se identificó que el servidor permitía **acceso anónimo** (sin autenticación), lo que exponía la estructura de directorios internos a cualquier actor externo, suponiendo un riesgo de fuga de información y un incumplimiento de las normativas de protección de datos. Aunque se verificó que los permisos de escritura estaban bloqueados (impidiendo la carga de malware), la exposición pública del servicio representaba un vector de ataque innecesario.

Estado de resolución: Se ha procedido a la **remediación inmediata** de la vulnerabilidad mediante el endurecimiento (hardening) de la configuración del servicio *vsftpd*, deshabilitando el acceso de usuarios invitados. Las pruebas de verificación posteriores confirman que el acceso no autorizado ha sido bloqueado exitosamente, restableciendo el nivel de seguridad del activo.

---

2. Alcance del Proyecto

- **Objetivo:** Servidor Linux Debian Hospital General de Madrid (ficticio).
- **IP Objetivo:** 192.168.122.10
- **Servicio Auditado:** Puerto 21(TCP)- Servicio FTP.
- **Herramientas Utilizadas:** `nmap`, cliente `ftp` de consola.
- **Tipo de Prueba:** Caja Gris (conocimiento parcial).

---

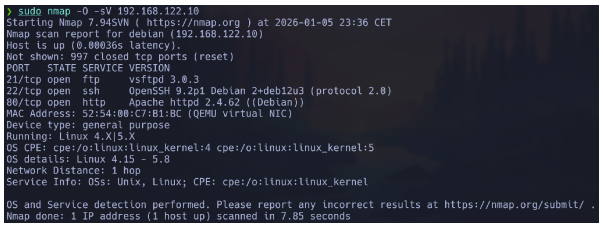
3. Detección de Vulnerabilidades (Reconocimiento)

Se realizó un escaneo en la máquina para detectar el posible servicio vulnerable.

Las pruebas arrojaron que el servicio FTP de transferencia de archivos estaba abierto y podía ser un vector de ataque para actores maliciosos.

A continuación, se muestra el proceso realizado de escaneo y detección de la vulnerabilidad:

- **Comando:** `nmap -O -sV 192.168.122.10`
  - `-O`: Escanea el sistema operativo y su versión.
  - `-sV`: Entrega los puertos abiertos y qué **software** (y qué versión) se está ejecutando en ese puerto.
- **Hallazgo:** Se detecta que el servicio FTP está abierto en el puerto 21 con `vsftpd 3.0.3`.
- **Interpretación:** El puerto FTP puede ser un vector de ataques común si se encuentra abierto y además posee una vulnerabilidad conocida como `ftp-anon`, la autenticación anónima que permite a los usuarios conectarse sin necesidad de nombre de usuario y contraseña específicos.
- **Captura del Escaneo a la máquina:**



Una vez detectado el servicio FTP abierto, se realiza un escaneo del puerto 21 para saber la versión junto con una prueba de scripts por defecto de *nmap* que realizará pruebas automáticamente en el servicio expuesto.

- **Comando:** `nmap -p 21 -sV -sC -vvv 192.168.122.10`
  - `-p 21`: Se especifica el puerto que se desea escanear.
  - `-sC`: Ejecución de scripts por defecto de `nmap` que realizará pruebas comunes en el servicio FTP.
  - `vvv`: Triple verbose, muestra los resultados del escaneo en tiempo real sin esperar a que finalice pudiendo así, parar la ejecución una vez encontrada la información relevante.
- **Hallazgo:** Se observa a continuación que, efectivamente, el servicio FTP cuenta con la vulnerabilidad **ftp-anon**.
- **Interpretación:** Con dicha vulnerabilidad, los **datos del servidor** del Hospital General de Madrid podrían verse expuestos o, en el peor de los casos, cargar un **archivo con código malicioso**.
- **Captura de la vulnerabilidad ftp-anon:**

```
PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.122.131
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
Service Info: OS: Unix
```

Detectado así el posible vector de ataque, se procede a la prueba de explotación del servicio FTP a través de la autenticación anónima `ftp-anon`.

---

4. Explotación (Prueba de Concepto)

Para la prueba de explotación, se usará la forma convencional para la entrada al servicio **FTP**. Sabiendo que, con `ftp-anon`, se puede usar el nombre de usuario **"anonymous"** y el campo de la contraseña vacío, accediendo y realizando pruebas de explotación.

- **Comando:** `ftp 192.168.122.10`
- **Uso:** Se accede al servicio FTP de la máquina con las credenciales:
  - **Usuario:** anonymous
  - **Contraseña:** (Se pulsa enter dejando el campo vacío)
- **Hallazgo:** Se accede al servicio FTP con las credenciales resultando exitoso.
- **Captura de entrada al servicio FTP:**

```
❯ ftp 192.168.122.10
Connected to 192.168.122.10.
220 (vsFTPd 3.0.3)
Name (192.168.122.10:isken): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Una vez realizada la autenticación, se procede a intentar subir un archivo de prueba llamado `test_seguridad.txt` para comprobar si el servicio permite la subida de archivos y, siendo así, una vulnerabilidad crítica para el Hospital.

- **Comando:** `put test_seguridad.txt`
- **Uso:** Intentará subir un archivo de texto y comprobar así los permisos.
- **Hallazgo:** Devuelve el código `550` que deniega la subida de archivos al servicio.
- **Captura de la denegación de subida de archivos:**

```
ftp> put test_seguridad.txt
local: test_seguridad.txt remote: test_seguridad.txt
229 Entering Extended Passive Mode (|||61320|)
550 Permission denied.
ftp>
```

Después de realizar la prueba y mostrar los permisos denegados al intentar transferir el archivo, se explicará a continuación, las medidas de corrección aplicadas para mitigar la vulnerabilidad de **exposición de datos sensibles**.

---

5. Medidas de Corrección (Hardening)

A continuación, se aplicarán las medidas adecuadas para mitigar/solucionar la vulnerabilidad de acceso anónimo al servicio FTP. Editando el archivo de configuración `/etc/vsftpd.conf` y cambiando los valores de `anonymous_enable=YES` a `anonymous_enable=NO`. Se mostrarán los pasos seguidos para la correcta configuración.

- **Comando:** `sudo nano /etc/vsftpd.conf`
- **Uso:** Usando el editor de texto `nano` se accede al archivo localizado en `/etc/` y así modificar con permisos de usuario privilegiado (root).
- Se busca la línea `anonymous_enable=YES`.
- **Captura de la línea:**

```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
```

- Y se cambia a `anonymous_enable=NO`.
- **Captura de la edición al valor NO:**

```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
```

Una vez realizados los cambios, se reinicia el servicio `vsftpd` para aplicarlos.

- **Comando:** `sudo systemctl restart vsftpd`

- **Captura del servicio reiniciado:**

```
debian@debian:~$ sudo systemctl restart vsftpd
```

Realizados los cambios y con el servicio reiniciado, se procede a hacer la verificación volviendo a repetir el proceso de entrada al servicio desde un usuario anónimo.

---

6. Verificación (Retesting)

En este punto, se realizarán los mismos pasos que en el punto **4. Explotación**, para verificar que el acceso del servicio FTP se ha revocado desde un usuario anónimo y que la vulnerabilidad se ha corregido de forma exitosa.

- **Comando:** `ftp 192.168.122.10`
  - Se usan las mismas credenciales de acceso que anteriormente permitieron las conexión con el servidor.
- **Hallazgo:** El servidor rechaza la conexión anónima.
- **Captura del servidor rechazando la conexión anónima:**

```
❯ ftp 192.168.122.10
Connected to 192.168.122.10.
220 (vsFTPd 3.0.3)
Name (192.168.122.10:isken): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
```

---

7. Conclusiones y Recomendaciones Finales

La vulnerabilidad de acceso anónimo ha sido mitigada exitosamente, eliminando el riesgo inmediato de fuga de información pública.

Sin embargo, como medida de mejora estratégica (Hardening avanzado), se recomienda a la organización planificar la **desactivación total del servicio FTP (Puerto 21)** a medio plazo. Dado que el servidor ya cuenta con SSH (Puerto 22) habilitado, se sugiere migrar los flujos de trabajo a **SFTP**, garantizando así que no solo la autenticación, sino también la transferencia de datos, viajen cifradas, alineándose con las mejores prácticas de seguridad (ISO 27001).