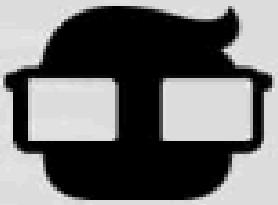


Pentesting Technical Report

4Geeks
Ph: +1 786 345 5555

INFORME DE PENTESTING - VULNERABILIDADES EN ENTORNO CONTROLADO

Target Principal: Servidor clave 192.168.1.152

Fecha de Ejecución: 10 de enero 2026

Autor: Aaron Jorge Climent

Versión: 1.0

ÍNDICE

1. ALCANCE DEL TRABAJO

Objetivos Principales

- Identificar vulnerabilidades críticas en el sistema del servidor clave.
- Explotar puertas traseras y servicios mal configurados.
- Evaluar postura de seguridad de aplicaciones web.
- Aplicar soluciones en el entorno de producción.

Limitaciones y Exclusiones

- No se probaron ataques de denegación de servicio (DoS).
- No se realizó fuzzing intensivo en aplicaciones web.
- No se explotaron vulnerabilidades físicas.
- No se probó ingeniería social.

Sistemas en Alcance

Objetivo: Servidor clave de una empresa de informática (192.168.1.152)

Atacante: 192.168.1.11 (Kali Linux 2025.4)

Herramientas: nmap, msf

2. RESUMEN EJECUTIVO

Como parte de la evaluación continua de seguridad en el Hospital General de Madrid, se realizó una auditoría de caja gris sobre el servidor crítico 192.168.122.10, con el propósito de detectar posibles vulnerabilidades que pudieran comprometer la confidencialidad de los datos.

Durante el análisis, se identificó una vulnerabilidad de severidad media en el servicio FTP, debido a que permitía acceso anónimo sin necesidad de autenticación. Esto exponía la estructura interna de directorios a cualquier actor externo, generando un riesgo de fuga de información y vulnerando las normativas de protección de datos. Aunque se constató que los permisos de escritura estaban bloqueados (evitando la carga de malware), la exposición pública del servicio constituía un vector de ataque innecesario.

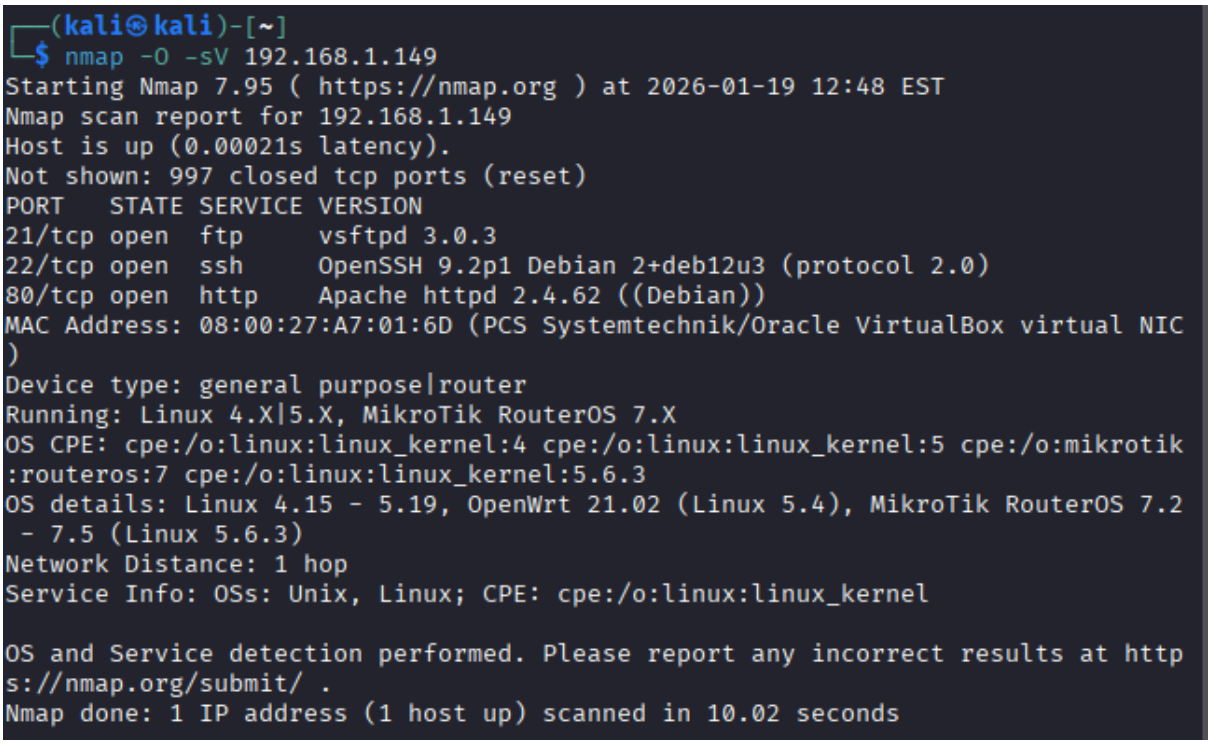
La vulnerabilidad fue mitigada de forma inmediata mediante el hardening de la configuración del servicio vsftpd, deshabilitando el acceso de usuarios invitados. Las pruebas posteriores confirmaron que el acceso no autorizado quedó bloqueado con éxito, restableciendo la seguridad del sistema.

3. Escaneo de Vulnerabilidades

Se llevó a cabo un escaneo en el sistema para identificar posibles servicios vulnerables. Los resultados indicaron que el servicio FTP de transferencia de archivos se encontraba abierto y podría constituir un vector de ataque para actores maliciosos.

-Comando: nmap -O -sV 192.168.1.149

Resultado:



-Se detectan los puertos 21, 22 y 80 abiertos.

-La versión de vsftpd 3.0.3 del puerto 21 indica una vulnerabilidad que conlleva el acceso de forma anónima, es decir, sin necesidad de usuario y contraseña.

-El puerto 80 no filtra el acceso por ip lo cual puede ser una vulnerabilidad ya que no bloquea por muchos intentos denegados de acceso

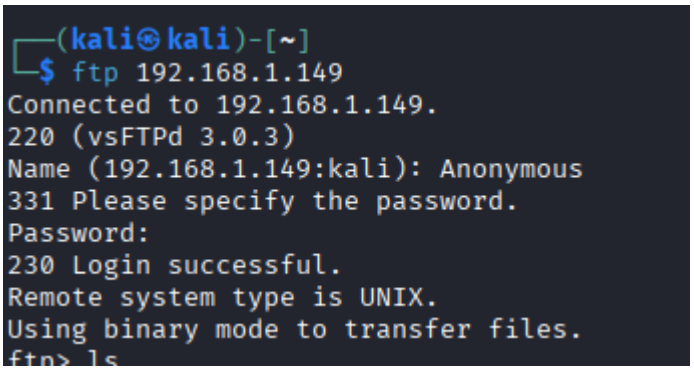
4. Explotación

Para la prueba de explotación, se empleará el método convencional de acceso al servicio FTP. Se sabe que, utilizando el modo ftp-anon, es posible acceder con el usuario "anonymous" y dejar la contraseña en blanco, permitiendo así realizar las pruebas de explotación.

-Comando: ftp 192.168.1.149

Y se usan las credenciales de “Anonymous” y se deja vacio la parte de contraseña

Resultado:



-Se demuestra que el acceso anónimo está permitido

5. Acciones Tomadas

Se instalo el plugin “iptables” con el comando:

-Comando: sudo apt-get install iptables

Se estableció unas reglas en el servidor Apache con Iptables que bloquean las ip entrantes que fallen el acceso por credenciales erroneas, y tambien se bloqueo el acceso remoto ssh

-Comandos:

Política predeterminada: permitir todo el tráfico saliente, bloquear todo el tráfico entrante

iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT ACCEPT

Permitir tráfico local (loopback)

```
iptables -A INPUT -i lo -j ACCEPT

# Permitir conexiones establecidas y relacionadas
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Denegar SSH
iptables -A INPUT -p tcp --dport 22 -j DROP

# Permitir tráfico HTTP y HTTPS desde tu red local
iptables -A INPUT -s 192.168.0.0/16 -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -s 192.168.0.0/16 -p tcp --dport 443 -j ACCEPT
# Crear una nueva cadena para manejar intentos fallidos
iptables -N LOG_AND_DROP

# Configurar la cadena para registrar y luego bloquear
iptables -A LOG_AND_DROP -j LOG --log-prefix "IP BLOCKED: " --log-level 4
iptables -A LOG_AND_DROP -j DROP

# Bloquear IPs después de 3 intentos fallidos en 60 segundos
iptables -A INPUT -p tcp --dport 80 -m recent --name http_failed --set
iptables -A INPUT -p tcp --dport 80 -m recent --name http_failed --update --seconds 60
--hitcount 3 -j LOG_AND_DROP
```

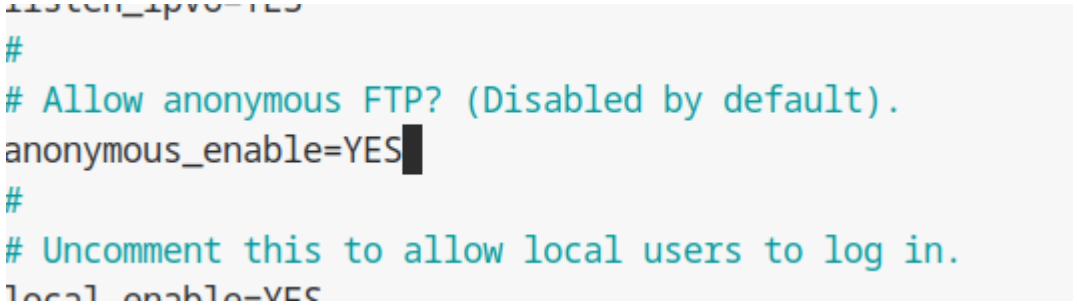
```
root@debian:~# # Limpiar reglas existentes
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X

# Política predeterminada: permitir todo el tráfico saliente, bloquear todo el t
ráfico entrante
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

# Permitir tráfico local (loopback)
iptables -A INPUT -i lo -j ACCEPT

# Permitir conexiones establecidas y relacionadas
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Denegar SSH
iptables -A INPUT -p tcp --dport 22 -j DROP

# Permitir tráfico HTTP y HTTPS desde tu red local
iptables -A INPUT -s 192.168.0.0/16 -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -s 192.168.0.0/16 -p tcp --dport 443 -j ACCEPT
```

```
root@debian:~# # Crear una nueva cadena para manejar intentos fallidos
iptables -N LOG_AND_DROP

# Configurar la cadena para registrar y luego bloquear
iptables -A LOG_AND_DROP -j LOG --log-prefix "IP BLOCKED: " --log-level 4
iptables -A LOG_AND_DROP -j DROP

# Bloquear IPs después de 3 intentos fallidos en 60 segundos
iptables -A INPUT -p tcp --dport 80 -m recent --name http_failed --set
iptables -A INPUT -p tcp --dport 80 -m recent --name http_failed --update --seco
nds 60 --hitcount 3 -j LOG_AND_DROP
root@debian:~#
```

A continuación, se procederá a tomar las medidas necesarias para corregir y reducir la vulnerabilidad de acceso anónimo en el servicio FTP. Para ello, se editará el archivo de configuración /etc/vsftpd.conf, modificando la opción anonymous_enable, pasando su valor de YES a NO. A lo largo de este proceso, se describirán detalladamente cada uno de los pasos realizados para asegurar que la configuración quede correcta y que el servicio deje de permitir conexiones abiertas de manera anónima.

-Comando: sudo nano /etc/vsftpd.conf

Una vez ejecutado se cambiara manualmente la configuración cambiando el parametro de “anonymous_enable” de “YES” a “NO”



6. RECOMENDACIONES

Se ha mitigado las vulnerabilidades encontradas a si que una de las recomendaciones principales seria no cambiar las configuraciones realizadas anteriormente sin un objetivo claro, se deberia desactivar el puerto 21 y seguir las medidas de seguridad que se explican en el documento ISO 27001

FIN DEL INFORME