

Detección y corrección de vulnerabilidades

Versión	Fecha	Autor	Descripción
v.01	04/06/2025	Luis F. Gómez Guzmán	Fase 2 Proyecto final

Índice

1. Objetivo y alcance	3
2. Herramientas y técnicas utilizadas	3
3. Resultados	3
4. Análisis.....	6
5. Explotación de vulnerabilidad	8
6. Conclusión y mitigación.....	11
7. Anexo I. Vulnerabilidades.....	15

1. Objetivo y alcance

El objetivo de este informe es detallar las vulnerabilidades de la máquina virtual Debian hackeada.

El alcance incluye la identificación de la dirección IP, los servicios y puertos expuestos, así como la detección y explotación de una de las vulnerabilidades encontradas.

2. Herramientas y técnicas utilizadas

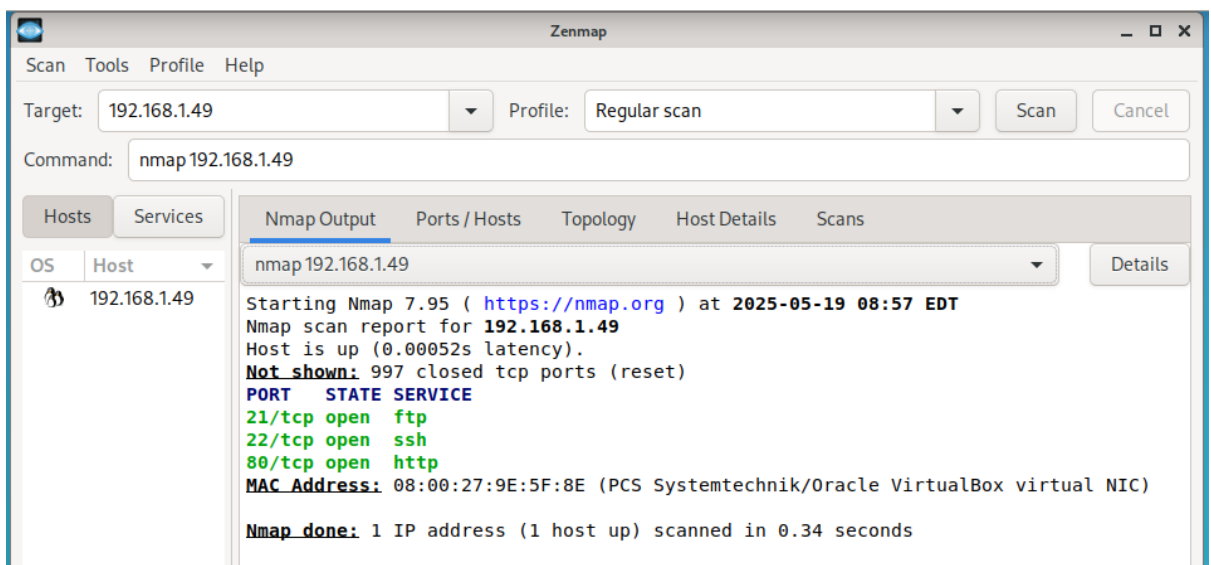
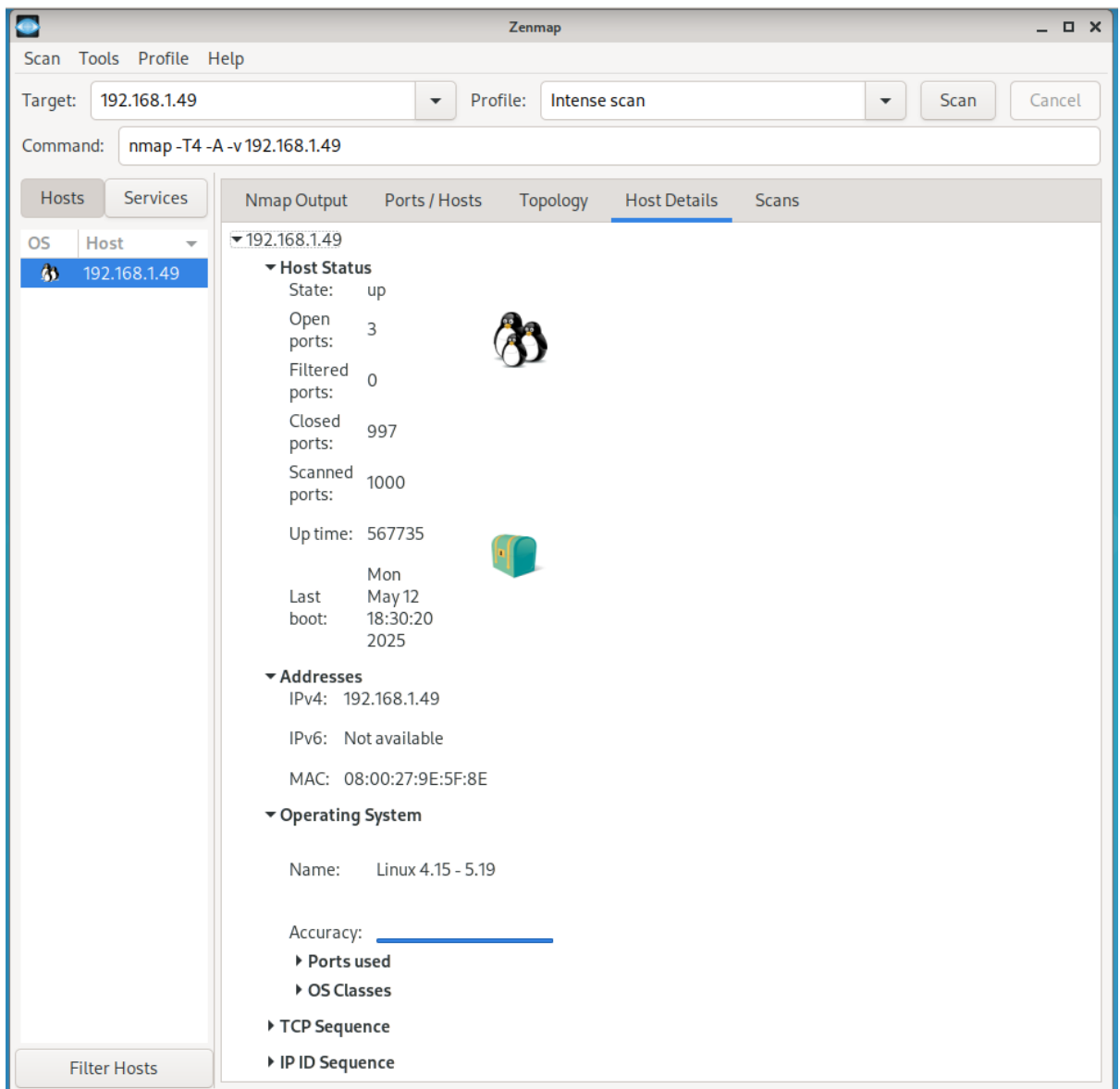
- **ip a:** Comando utilizado en la máquina Debian para identificar la dirección IP.
- **Nmap – Zenmap** (Network Mapper): Herramienta de análisis de redes utilizada en Kali Linux para realizar el escaneo de las vulnerabilidades.
 - ✱ **nmap -T4 -A -v 192.168.1.49:** Comando para ejecutar un escaneo profundo y rápido sobre la dirección IP 192.168.1.49
 - **-T4:** Ajusta la agresividad del escaneo. T4 indica una configuración rápida, lo que significa que nmap realizará la exploración con menor latencia y mayor velocidad.
 - **-A:** Activa funciones avanzadas de detección, incluyendo: a) Detección del sistema operativo; b) Identificación de servicios y versiones; c) Búsqueda de scripts y huellas digitales.
 - **-v:** Modo detallado (verbose). Proporciona más información sobre el progreso del escaneo.
 - **192.168.1.49:** Es la dirección IP del objetivo que se va a escanear.
- **Wireshark:** Analizador de protocolos de red que permite capturar y examinar en detalle el tráfico que circula por una red informática.
- **hping3:** Herramienta de línea de comandos para generar y analizar paquetes personalizados en redes.

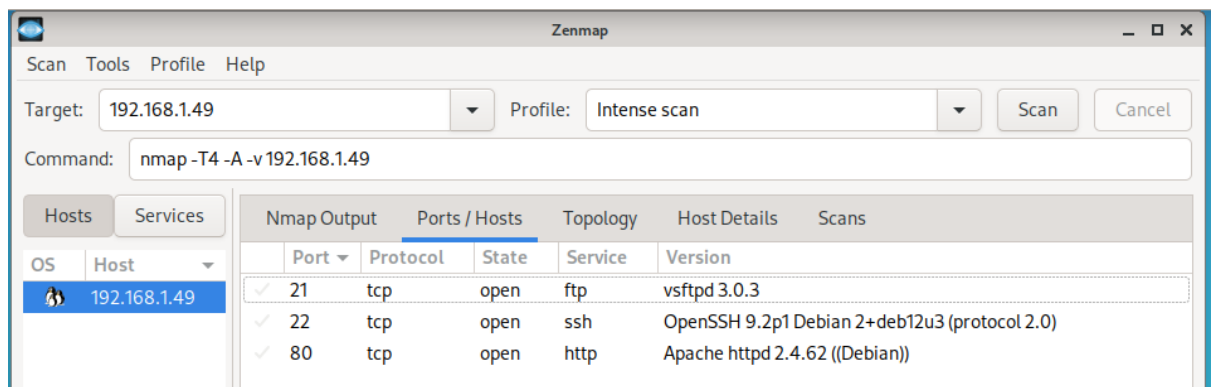
3. Resultados

A) Dirección IP y puertos abiertos

Dirección IP de Debian: 192.168.1.49

```
debian@debian: ~  
File Edit View Search Terminal Help  
debian@debian:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:9e:5f:8e brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.49/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3  
        valid_lft 86371sec preferred_lft 86371sec  
    inet6 fd65:2e4:8f79:8547:e40e:2be5:8638:341/64 scope global temporary dynamic  
    inet6 fd65:2e4:8f79:8547:a00:27ff:fe9e:5f8e/64 scope global dynamic mngtmpdr noprefixroute  
        valid_lft 1774sec preferred_lft 1774sec  
    inet6 fe80::a00:27ff:fe9e:5f8e/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
debian@debian:~$
```

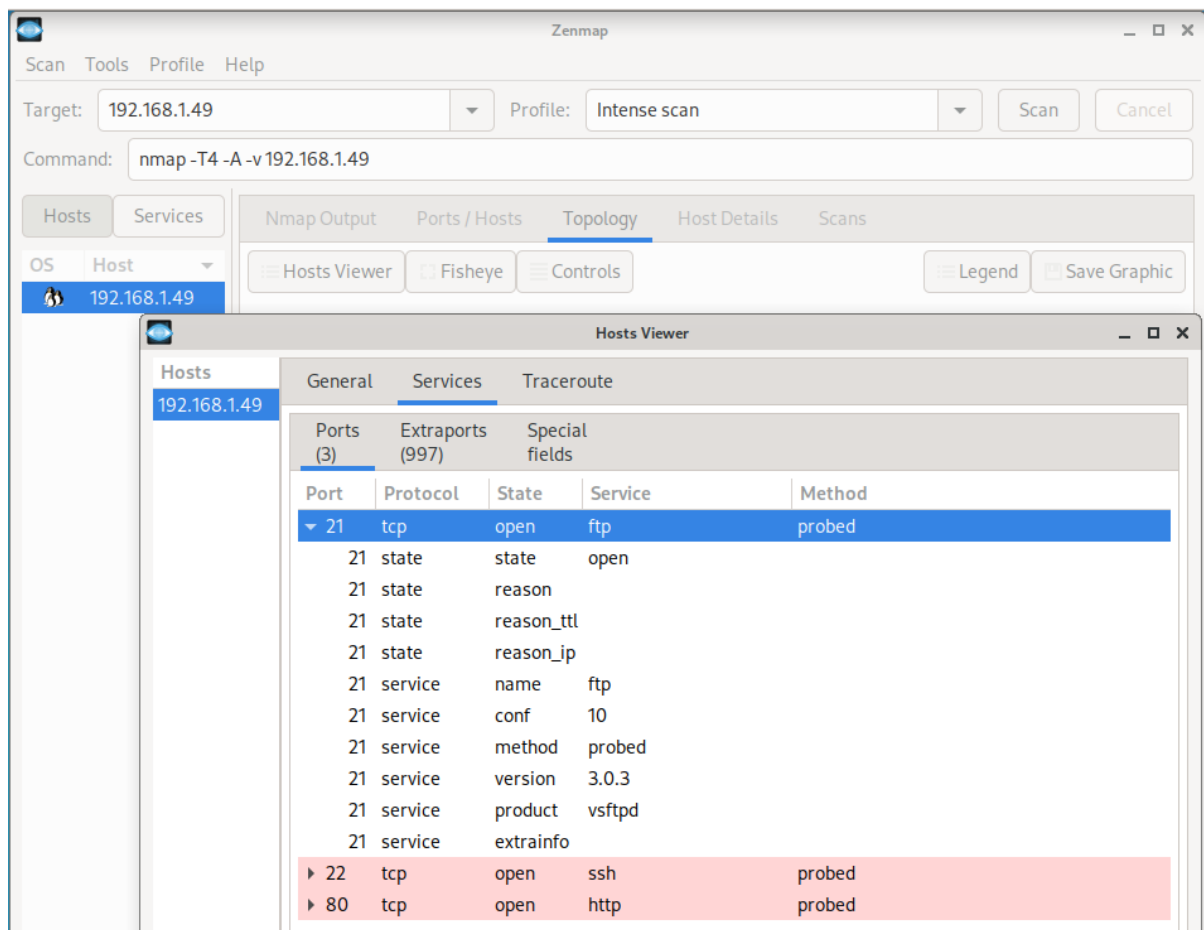




B) Escaneo de vulnerabilidades¹

4. Análisis

- vsftpd 3.0.3 (FTP):

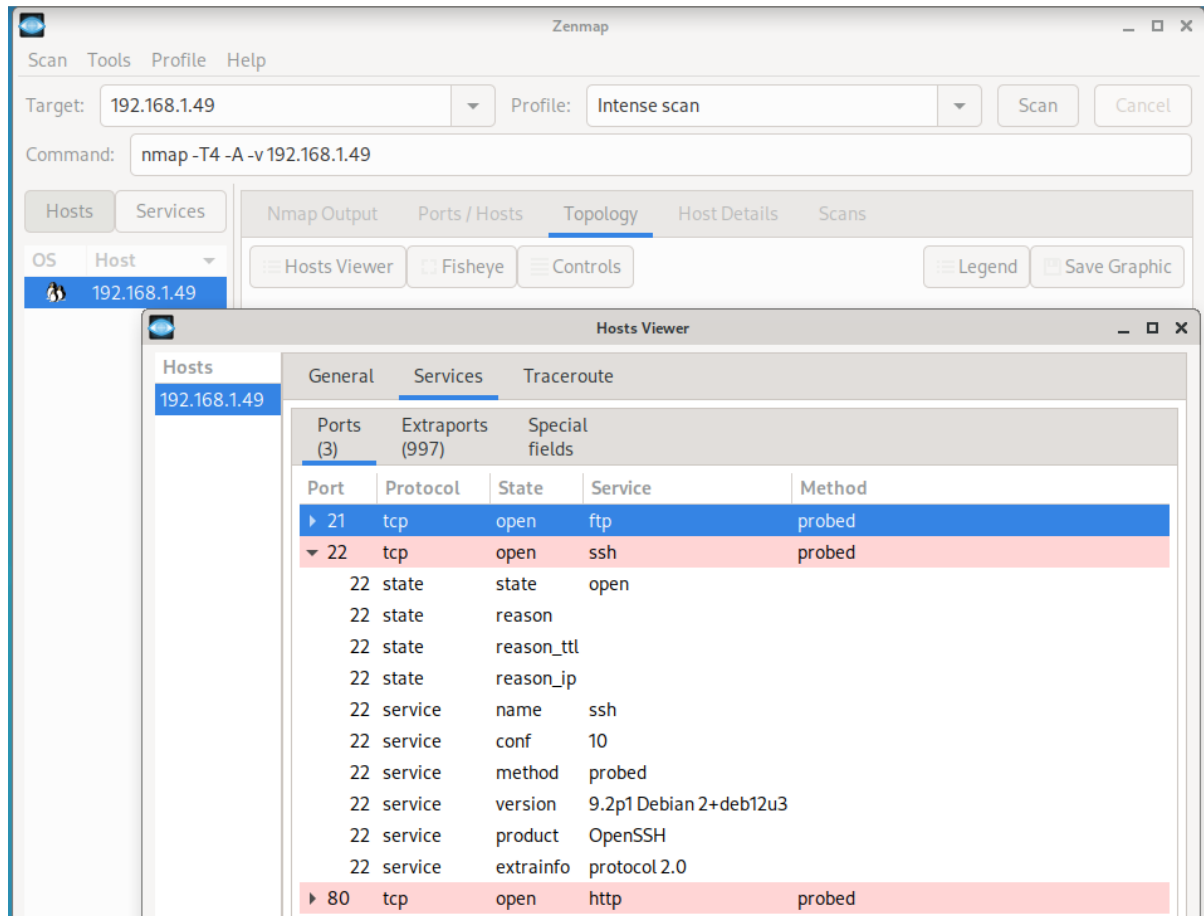


Vulnerabilidad: VSFTPD 3.0.3 permite a los atacantes provocar una denegación de servicio debido al número limitado de conexiones permitidas.

¹ Ver Anexo I. Vulnerabilidades (capturas del escaneo intenso 192.168.1.49).

CVE: [CVE-2021-30047](#)

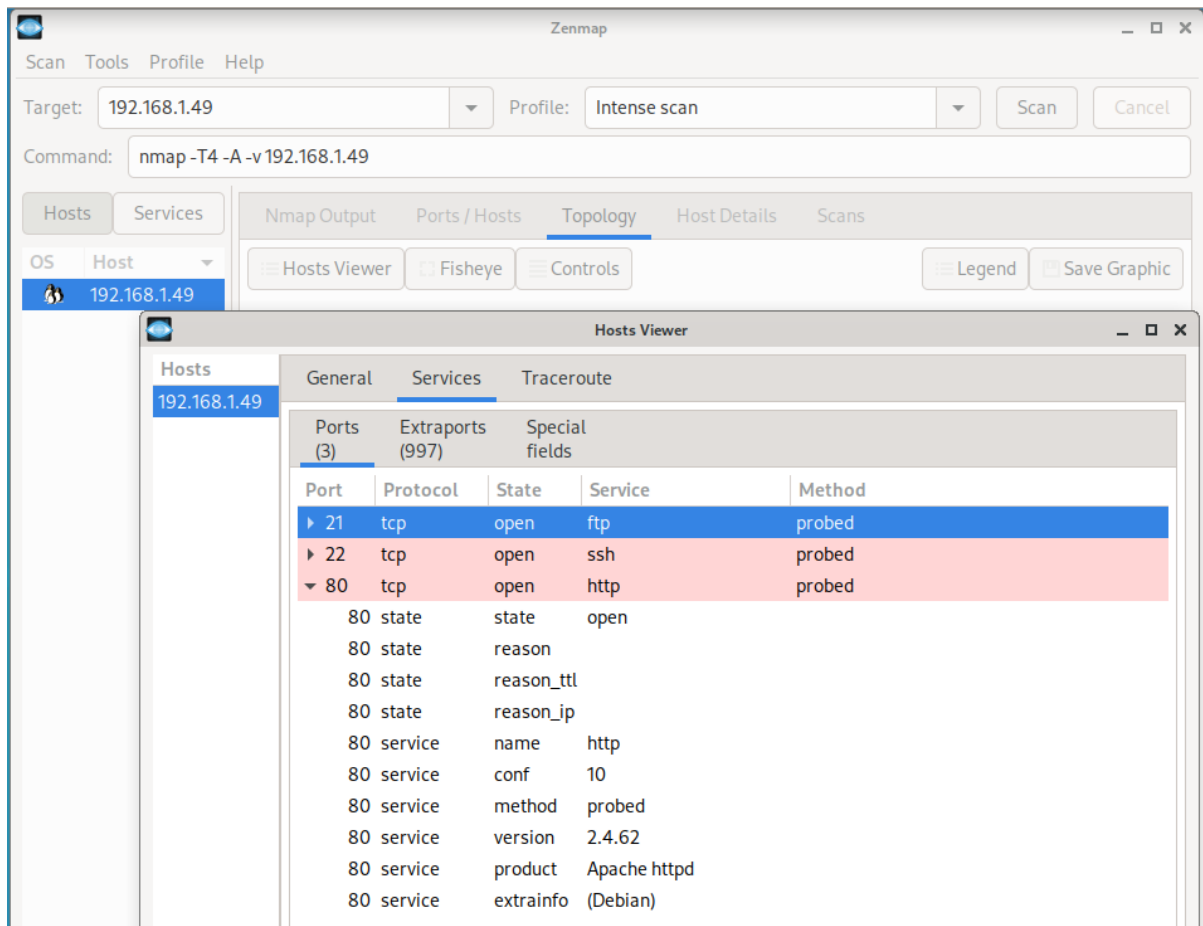
- **OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)**



Vulnerabilidad: Se ha descubierto una regresión de seguridad (CVE-2006-5051) en el servidor de OpenSSH (sshd). Existe una condición de carrera que puede llevar a sshd a manejar algunas señales de forma insegura. Un atacante remoto no autenticado puede ser capaz de desencadenarla al no autenticarse dentro de un periodo de tiempo establecido

CVE: [CVE-2024-6387](#)

- **Apache httpd 2.4.62 ((Debian))**



Vulnerabilidad: Por el momento no hay vulnerabilidades.

CVE: [CVE-2024-40725](https://www.cve.org/CVERecord?id=CVE-2024-40725)

Otras bases de datos:

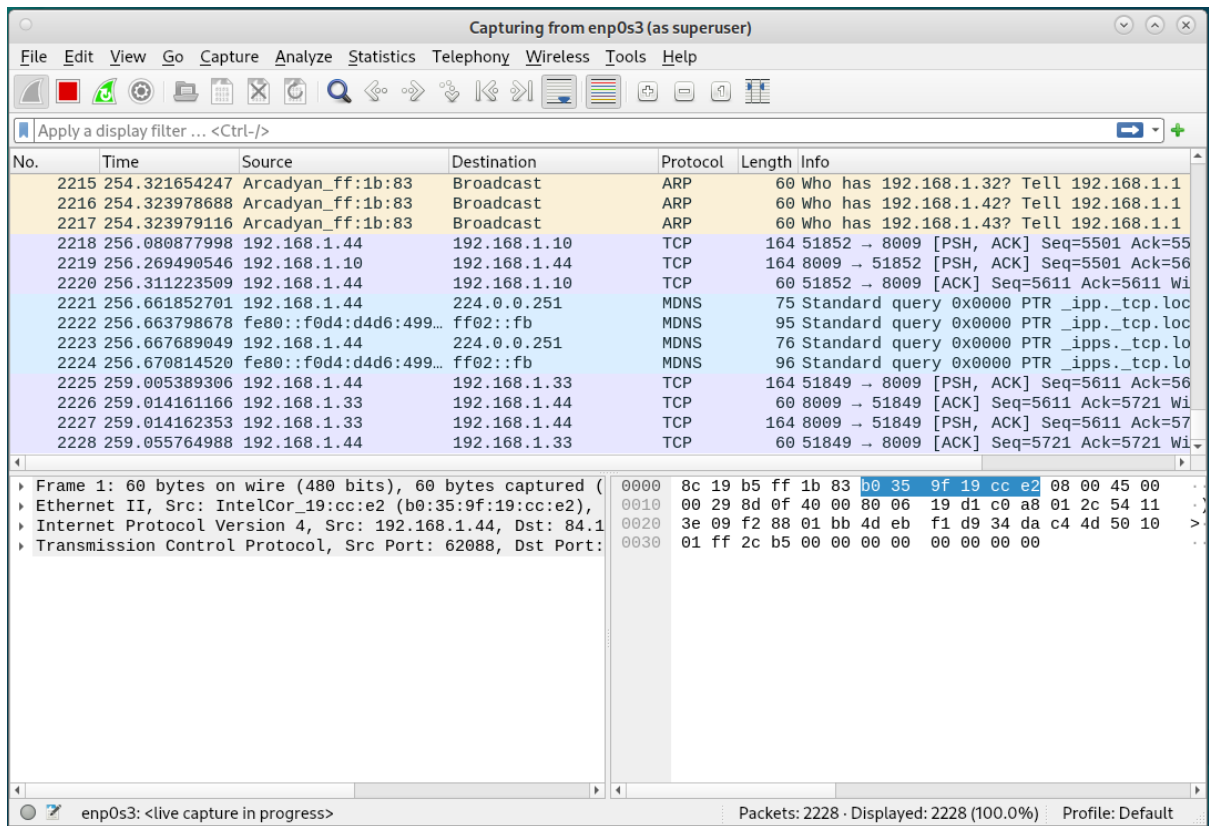
- https://httpd.apache.org/security/vulnerabilities_24.html.
- <https://www.cve.org/CVERecord?id=CVE-2024-40725>
- <https://www.cvedetails.com/version/1801384/Apache-Http-Server-2.4.62.html>

5. Explotación de vulnerabilidad

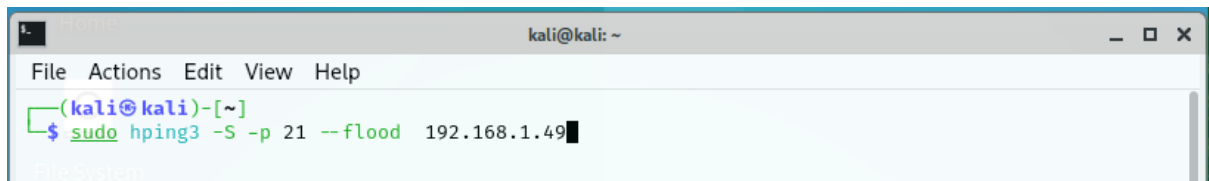
- ✖ Explotación de vulnerabilidad en el servicio FTP [ataque de denegación de servicio (DDoS)]

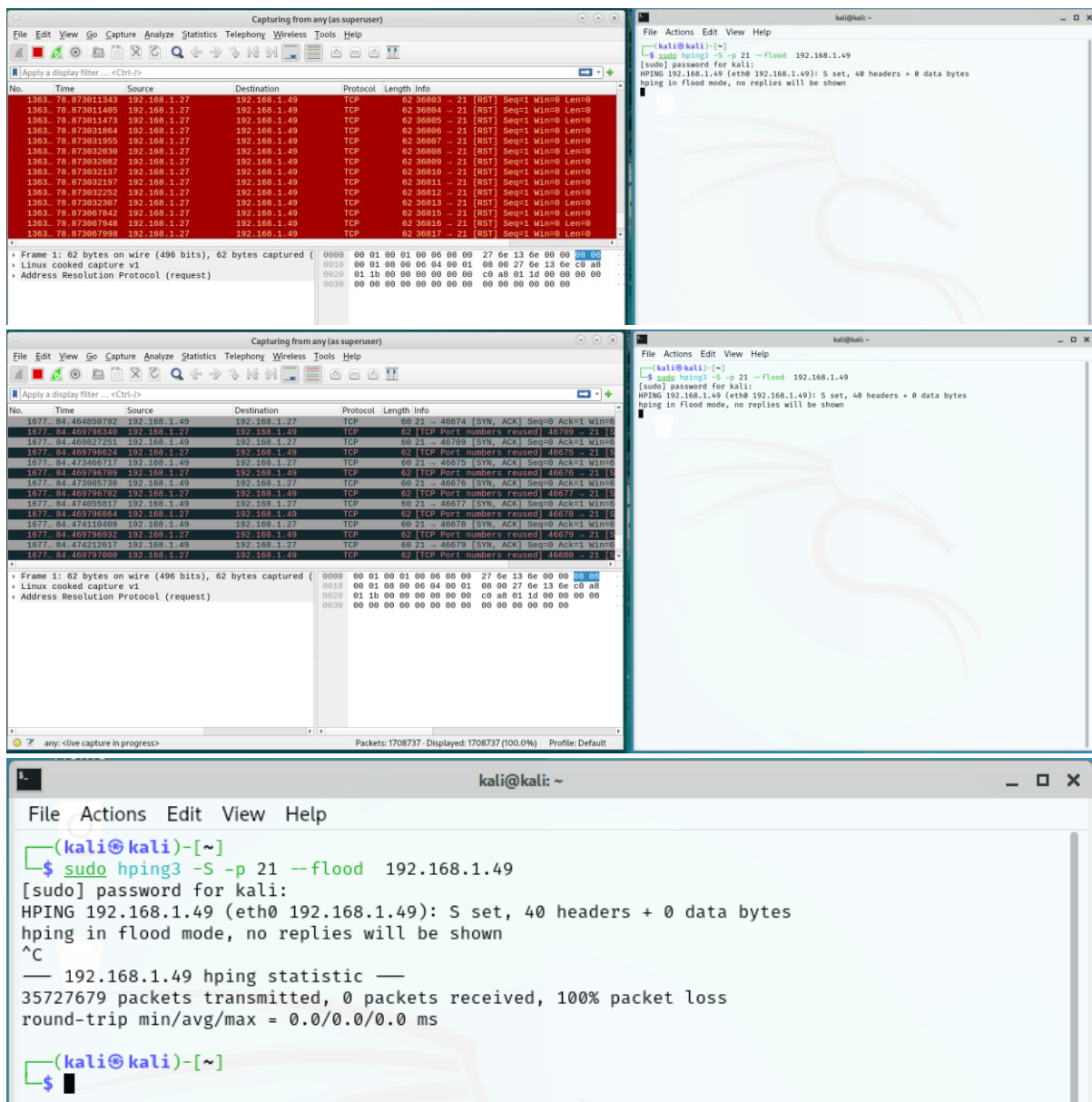
1. Instalación de Wireshark en la máquina virtual Debian hackeada


```
debian@debian: ~  
File Edit View Search Terminal Help  
debian@debian:~$ sudo apt install wireshark  
[sudo] password for debian:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  libbcg729-0 libc-ares2 libdouble-conversion3 liblua5.2-0 libmd4c0 libminizip1  
  libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5multimedia5  
  libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5  
  libqt5network5 libqt5printsupport5 libqt5qml5 libqt5qmlmodels5 libqt5quick5  
  libqt5svg5 libqt5waylandclient5 libqt5waylandcompositor5 libqt5widgets5 libsmi2ldbl  
  libwireshark-data libwireshark16 libwiretap13 libwsutil14 libxcb-icccm4  
Processing triggers for desktop-file-utils (0.26-1) ...  
Processing triggers for hicolor-icon-theme (0.17-2) ...  
Processing triggers for mate-menus (1.26.0-3) ...  
Processing triggers for libc-bin (2.36-9+deb12u10) ...  
debian@debian:~$ wireshark --version  
Wireshark 4.0.17 (Git v4.0.17 packaged as 4.0.17-0+deb12u1).  
  
Copyright 1998-2024 Gerald Combs <gerald@wireshark.org> and contributors.  
Licensed under the terms of the GNU General Public License (version 2 or later).  
This is free software; see the file named COPYING in the distribution. There is  
NO WARRANTY; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  
  
Compiled (64-bit) using GCC 12.2.0, with GLib 2.74.6, with PCRE2, with zlib  
1.2.13, with Qt 5.15.8, with libpcap, with POSIX capabilities (Linux), with  
libnl 3, with Lua 5.2.4, with GnuTLS 3.7.9 and PKCS #11 support, with Gcrypt  
1.10.1, with Kerberos (MIT), with MaxMind, with nghttp2 1.52.0, with brotli,  
with LZ4, with Zstandard, with Snappy, with libxml2 2.9.14, with libsmi 0.4.8,  
with QtMultimedia, without automatic updates, with SpeexDSP (using system  
library), with Minizip, with binary plugins.  
  
Running on Linux 6.1.0-37-amd64, with Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz  
(with SSE4.2), with 1967 MB of physical memory, with GLib 2.74.6, with PCRE2  
10.42 2022-12-11, with zlib 1.2.13, with Qt 5.15.8, with libpcap 1.10.3 (with  
TPACKET_V3), with c-ares 1.18.1, with GnuTLS 3.7.9, with Gcrypt 1.10.1, with  
nghttp2 1.52.0, with brotli 1.0.9, with LZ4 1.9.4, with Zstandard 1.5.4, with  
libsmi 0.4.8, with LC_TYPE=en_US.UTF-8, binary plugins supported.  
debian@debian:~$
```



2. Lanzamiento del ataque en Kali





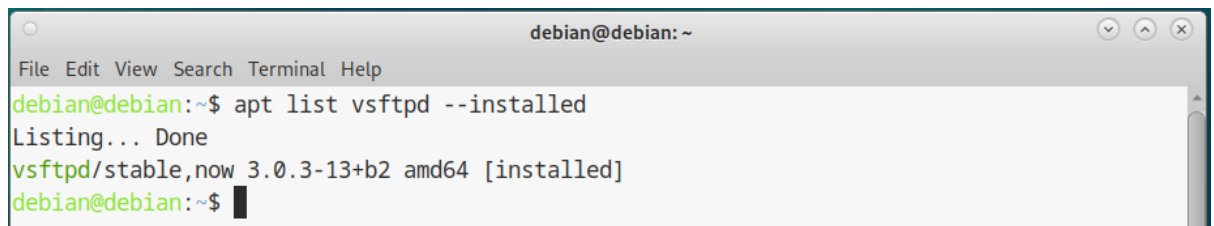
Después de llevarse a cabo el ataque de DDoS, Debian experimenta una notable disminución en el rendimiento, seguido de una total inutilización del sistema. La respuesta a comandos y solicitudes se vuelve inexistente, llegando incluso a producirse un bloqueo absoluto.

Este tipo de ataque no sólo compromete la operatividad del sistema, sino que también puede afectar a la estabilidad de los servicios alojados en la máquina, causando interrupciones prolongadas y posibles daños en la integridad de los datos. Además, la sobrecarga generada puede impactar negativamente en otros recursos de la red, ralentizando el funcionamiento general y dificultando la recuperación sin una mitigación adecuada.

6. Conclusión y mitigación

Con motivo de los resultados obtenidos, se recomienda tomar medidas para fortalecer y mejorar la seguridad como:

→ Actualizar el servicio (FTP)



```
debian@debian: ~  
File Edit View Search Terminal Help  
debian@debian:~$ apt list vsftpd --installed  
Listing... Done  
vsftpd/stable,now 3.0.3-13+b2 amd64 [installed]  
debian@debian:~$
```

→ **Proteger el servicio (FTP) en el puerto 21** contra **ataques de DDoS** utilizando **iptables**, de tal modo que aplicando reglas se pueda limitar la frecuencia de conexiones nuevas, detectar y bloquear las direcciones sospechosas y mitigar el tráfico malicioso. Así, en concreto:

A. Reglas

1. Limitar las tasas de conexión nuevas

```
iptables -A INPUT -p tcp --dport 21 -m connlimit --connlimit-above 5 -j DROP
```

- Evita múltiples intentos de conexión excesivos desde la misma IP en un corto período
- Bloquea cualquier IP que establezca más de 5 conexiones simultáneas al puerto 21

2. Limitar la cantidad de intentos por segundo

```
iptables -A INPUT -p tcp --dport 21 -m limit --limit 3/sec --limit-burst 5 -j  
ACCEPT  
iptables -A INPUT -p tcp --dport 21 -j DROP
```

- Permite un máximo de 3 intentos de conexión por segundo
- Impide ataques de tipo brute-force o sobrecarga masiva

3. Detectar y bloquear IPs sospechosas con recent

```
iptables -A INPUT -p tcp --dport 21 -m recent --set --name FTP  
iptables -A INPUT -p tcp --dport 21 -m recent --update --seconds 60 --hitcount 10  
--name FTP -j DROP
```

- Bloquea una IP si intenta conectarse demasiadas veces en un corto período
- Deniega el acceso si hay más de 10 intentos en 60 segundos

4. Bloquear direcciones IP maliciosas o sospechosas

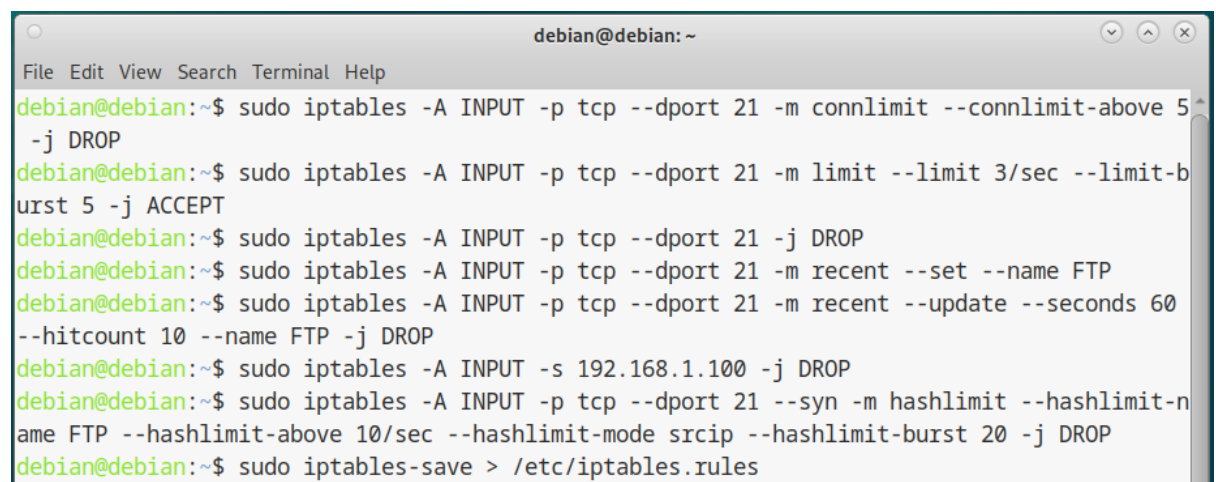
```
iptables -A INPUT -s 192.168.1.100 -j DROP
```

- Ejemplo de bloqueo manual de una IP

5. Habilitar reglas de SYN-flood protection

```
iptables -A INPUT -p tcp --dport 21 --syn -m hashlimit --hashlimit-name FTP --hashlimit-above 10/sec --hashlimit-mode srcip --hashlimit-burst 20 -j DROP
```

- Protege contra ataques de inundación SYN que buscan saturar el servicio



```
debian@debian: ~  
File Edit View Search Terminal Help  
debian@debian:~$ sudo iptables -A INPUT -p tcp --dport 21 -m connlimit --connlimit-above 5 -j DROP  
debian@debian:~$ sudo iptables -A INPUT -p tcp --dport 21 -m limit --limit 3/sec --limit-burst 5 -j ACCEPT  
debian@debian:~$ sudo iptables -A INPUT -p tcp --dport 21 -j DROP  
debian@debian:~$ sudo iptables -A INPUT -p tcp --dport 21 -m recent --set --name FTP  
debian@debian:~$ sudo iptables -A INPUT -p tcp --dport 21 -m recent --update --seconds 60 --hitcount 10 --name FTP -j DROP  
debian@debian:~$ sudo iptables -A INPUT -s 192.168.1.100 -j DROP  
debian@debian:~$ sudo iptables -A INPUT -p tcp --dport 21 --syn -m hashlimit --hashlimit-name FTP --hashlimit-above 10/sec --hashlimit-mode srcip --hashlimit-burst 20 -j DROP  
debian@debian:~$ sudo iptables-save > /etc/iptables.rules
```

B. Guardado de las reglas actuales para su persistencia tras el reinicio del sistema

```
debian@debian: ~  
File Edit View Search Terminal Help  
debian@debian:~$ sudo apt install iptables-persistent  
[sudo] password for debian:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  netfilter-persistent  
The following NEW packages will be installed:  
  iptables-persistent netfilter-persistent  
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.  
Need to get 16.4 kB of archives.  
After this operation, 89.1 kB of additional disk space will be used.  
Do you want to continue? [Y/n] Y  
Get:1 http://deb.debian.org/debian bookworm/main amd64 netfilter-persistent all 1.0.20 [7,384 B]  
Get:2 http://deb.debian.org/debian bookworm/main amd64 iptables-persistent all 1.0.20 [9,000 B]  
Fetched 16.4 kB in 0s (110 kB/s)  
Preconfiguring packages ...  
Configuring iptables-persistent  
-----
```

```
debian@debian: ~  
File Edit View Search Terminal Help  
Save current IPv6 rules? [yes/no] yes  
  
Selecting previously unselected package netfilter-persistent.  
(Reading database ... 171206 files and directories currently installed.)  
Preparing to unpack .../netfilter-persistent_1.0.20_all.deb ...  
Unpacking netfilter-persistent (1.0.20) ...  
Selecting previously unselected package iptables-persistent.  
Preparing to unpack .../iptables-persistent_1.0.20_all.deb ...  
Unpacking iptables-persistent (1.0.20) ...  
Setting up netfilter-persistent (1.0.20) ...  
Created symlink /etc/systemd/system/iptables.service → /lib/systemd/system/netfilter-persistent.service.  
Created symlink /etc/systemd/system/ip6tables.service → /lib/systemd/system/netfilter-persistent.service.  
Created symlink /etc/systemd/system/multi-user.target.wants/netfilter-persistent.service → /lib/systemd/system/netfilter-persistent.service.  
Setting up iptables-persistent (1.0.20) ...  
Processing triggers for man-db (2.11.2-2) ...  
debian@debian:~$ sudo netfilter-persistent save  
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save  
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save  
debian@debian:~$ sudo systemctl enable netfilter-persistent  
Synchronizing state of netfilter-persistent.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable netfilter-persistent  
debian@debian:~$
```

```

debian@debian:~$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source               destination
 0      0 DROP        6  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:21 #conn src/32 > 5
 0      0 ACCEPT      6  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:21 limit: avg 3/sec burst 5
 0      0 DROP        6  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:21
 0      0           6  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:21 recent: SET name: FTP sid
e: source mask: 255.255.255.255
 0      0 DROP        6  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:21 recent: UPDATE seconds: 6
0 hit_count: 10 name: FTP side: source mask: 255.255.255.255
 0      0 DROP        0  --  *      *       192.168.1.100        0.0.0.0/0
 0      0 DROP        6  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:21 flags:0x17/0x02 limit: ab
ove 10/sec burst 20 mode srcip

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source               destination
debian@debian:~$

```

C. Otras recomendaciones:

- + Utilizar Fail2Ban para mejorar la protección contra intentos repetitivos
- + Configurar TCP Wrappers (/etc/hosts.allow y /etc/hosts.deny) para restringir accesos
- + Limitar los rangos de IP permitidos si el servicio FTP sólo debe ser accesible dentro de ciertas redes

7. Anexo I. Vulnerabilidades

