

Vulnerabilidades detectadas en un servidor debian luego de un escaneo con Nmap con el siguiente comando **nmap -sV --script=vuln 192.168.1.37**

```
(kali㉿kali)-[~]
$ nmap -sV --script=vuln 192.168.1.37
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 04:36 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.1.37
Host is up (0.0026s latency).
Not shown: 999 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
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 43.45 seconds

(kali㉿kali)-[~]
$ nmap -sV 192.168.1.37
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 04:38 EDT
Nmap scan report for 192.168.1.37
Host is up (0.0025s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds

(kali㉿kali)-[~]
└─
```

Se ha encontrado la siguiente vulnerabilidad por el puerto 21/tcp ftp el cual está abierto y nos revela lo que se ejecuta por ese puerto

vsftpd 3.0.3

PUERTO	SERVICIO	VERSIÓN	VULNERABILIDAD	REFERENCIA
21	FTP	VSFTPD 3.0.3	Permite a atacantes provocar una denegación de servicio debido al número	https://nvd.nist.gov/vuln/detail/CVE-2021-30047

			limitado de conexiones permitidas.	
--	--	--	------------------------------------	--