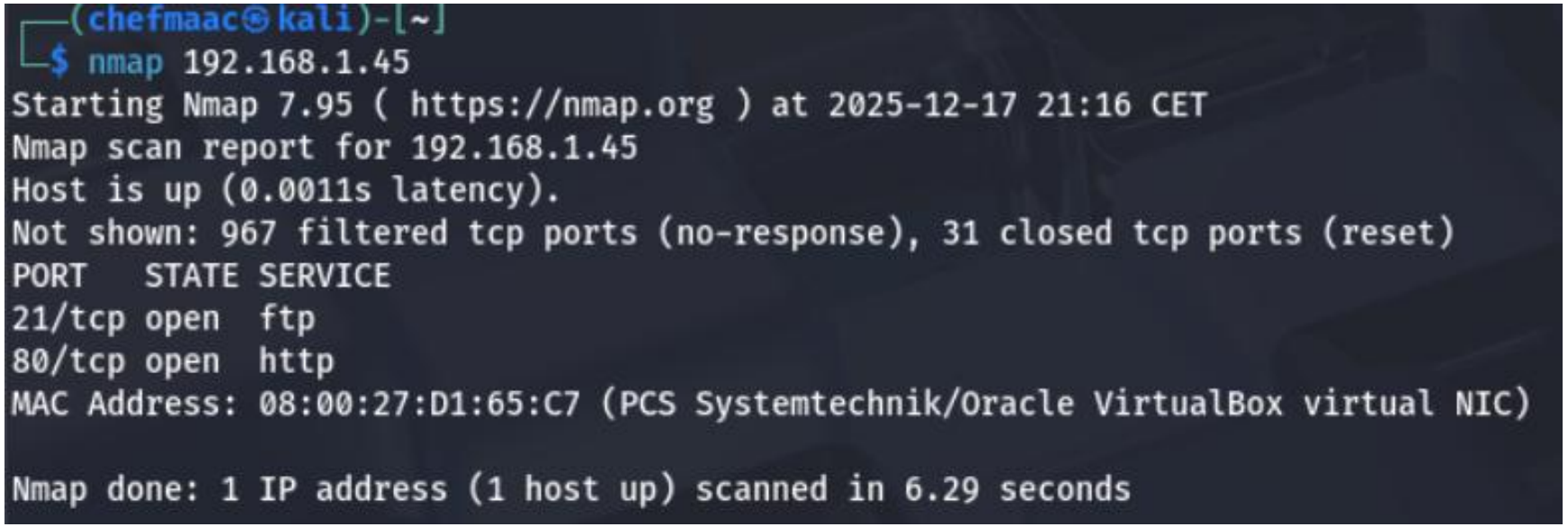
Análisis de vulnerabilidades

En el siguiente ejercicio analizaremos las vulnerabilidades de nuestra maquina Debian y los puestos abiertos.

El primer paso será analizas que puerto están abiertos. Lo hacemos con el código $nmap y el ip debian.

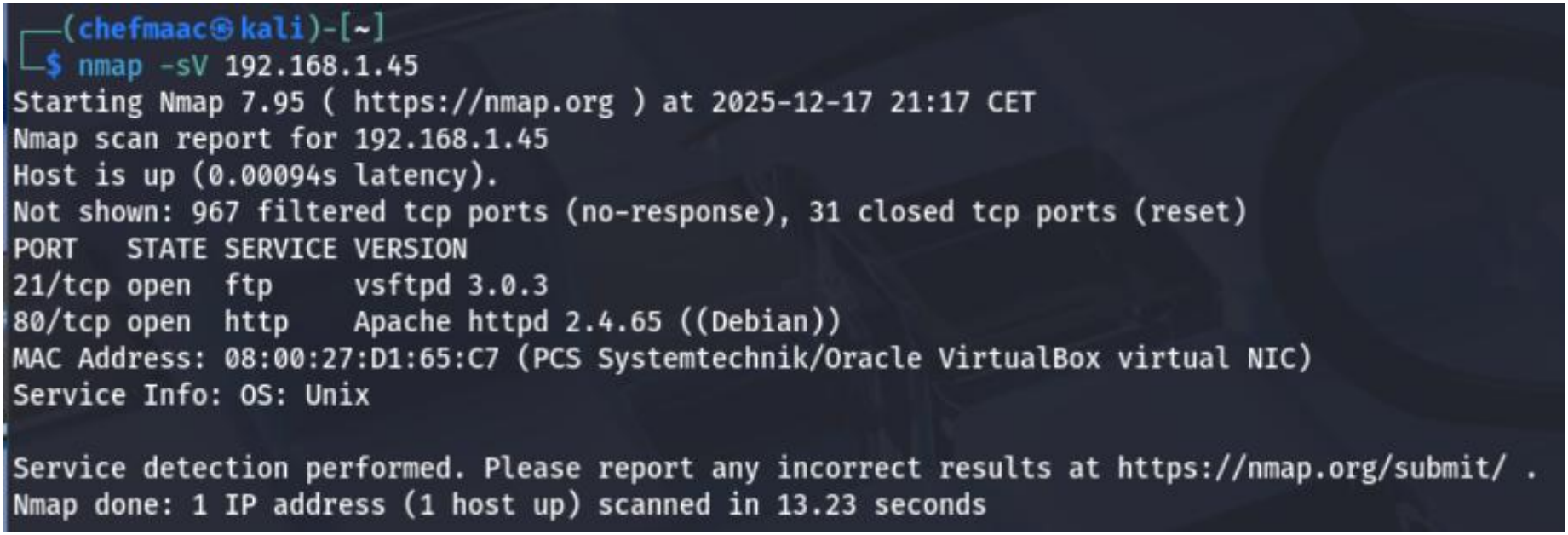
Puertos Abiertos



Podemos ver que existen 2 puertos abiertos y el servicio.

Puertos Abiertos y Servicios

El siguiente paso será verificar la versión de los puertos abiertos con el código $ nmap -sV y el ip de debian.



Podemos ver que los puertos abiertos tienen las versiones 21/tcp “vsftpd 3.0.3” y el 80/tcp “Apache httpd 2.4.65”

Puertos Abiertos y Vulnerabilidades

Para el siguiente paso del reporte, realizaremos un análisis de vulnerabilidades, en el podemos ver que los 2 puertos abiertos hay más de 1 vulnerabilidad.

```
└─$ nmap -sV --script=vuln 192.168.1.45
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 21:18 CET
Pre-scan script results:
|_broadcast-avahi-dos: ERROR: Script execution failed (use -d to debug)
Nmap scan report for 192.168.1.45
Host is up (0.0014s latency).
Not shown: 967 filtered tcp ports (no-response), 31 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-libopie:
|   VULNERABLE:
|   OPIE off-by-one stack overflow
|     State: LIKELY VULNERABLE
|     IDs:  BID:40403  CVE:CVE-2010-1938
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       An off-by-one error in OPIE library 2.4.1-test1 and earlier, allows remote
|       attackers to cause a denial of service or possibly execute arbitrary code
|       via a long username.
|     Disclosure date: 2010-05-27
|     References:
|       https://www.securityfocus.com/bid/40403
|       http://site.pi3.com.pl/adv/libopie-adv.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1938
|_      http://security.freebsd.org/advisories/FreeBSD-SA-10:05.opie.asc
| 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
```

```
80/tcp open  http    Apache httpd 2.4.65 ((Debian))
| vulners:
|   cpe:/a:apache:http_server:2.4.65:
|       CVE-2025-58098  8.3     https://vulners.com/cve/CVE-2025-58098
|       CNVD-2025-30564 8.3     https://vulners.com/cnvd/CNVD-2025-30564
|       CVE-2025-59775  7.5     https://vulners.com/cve/CVE-2025-59775
|       CVE-2025-55753  7.5     https://vulners.com/cve/CVE-2025-55753
|       CVE-2025-65082  6.5     https://vulners.com/cve/CVE-2025-65082
|_      CVE-2025-66200  5.4     https://vulners.com/cve/CVE-2025-66200
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache/2.4.65 (Debian)
| http-enum:
|   /wordpress/: Blog
|_  /wordpress/wp-login.php: Wordpress login page.
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 44.56 seconds
```

Tabla de Reporte de puertos y vulnerabilidades.

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
21	ftp	vsftpd 3.0.3	CVE-2010-1938	Error off-by-one en la librería OPIE (≤ 2.4.1-test1) que permite a un atacante remoto provocar DoS o posible ejecución de código enviando un nombre de usuario largo durante la autenticación FTP. Riesgo alto (CVSS 9.3).	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1938
21	ftp	vsftpd 3.0.3	CVE-2021-30047	Vulnerabilidad reportada en vsftpd que puede permitir comprometer la seguridad del servicio FTP dependiendo de la configuración.	https://vulners.com/cve/CVE-2021-30047
21	ftp	vsftpd 3.0.3	CVE-2021-3618	Falla de seguridad en vsftpd relacionada con el manejo de sesiones que puede facilitar ataques de denegación de servicio.	https://vulners.com/cve/CVE-2021-3618
80	HTTP	Apache httpd 2.4.65	CVE-2025-58098	Vulnerabilidad crítica en Apache HTTP Server que puede permitir acceso no autorizado o ejecución de acciones maliciosas dependiendo de la configuración del servidor.	https://vulners.com/cve/CVE-2025-58098
80	HTTP	Apache httpd 2.4.65	CNVD-2025-30564	Las versiones de Apache Web Server anteriores a **2.4.66** contienen una vulnerabilidad de inyección de comandos en el módulo **mod_cgid**, provocada por el	https://vulners.com/cnvd/CNVD-2025-30564

				manejo incorrecto de consultas escapadas para shell.	
80	HTTP	Apache httpd 2.4.65	CVE-2025-59775	Fallo de seguridad en Apache relacionado con el manejo de peticiones HTTP, con impacto potencial en confidencialidad e integridad.	https://vulners.com/cve/CVE-2025-59775
80	HTTP	Apache httpd 2.4.65	CVE-2025-55753	Vulnerabilidad que podría ser explotada para afectar la disponibilidad o seguridad del servidor web Apache.	https://vulners.com/cve/CVE-2025-55753
80	HTTP	Apache httpd 2.4.65	CVE-2025-65082	Falla de severidad media que afecta al servidor Apache HTTP en determinadas configuraciones.	https://vulners.com/cve/CVE-2025-65082
80	HTTP	Apache httpd 2.4.65	CVE-2025-66200	Vulnerabilidad de bajo a medio impacto que puede comprometer la seguridad del servidor web.	https://vulners.com/cve/CVE-2025-66200