Vulnerabilities report

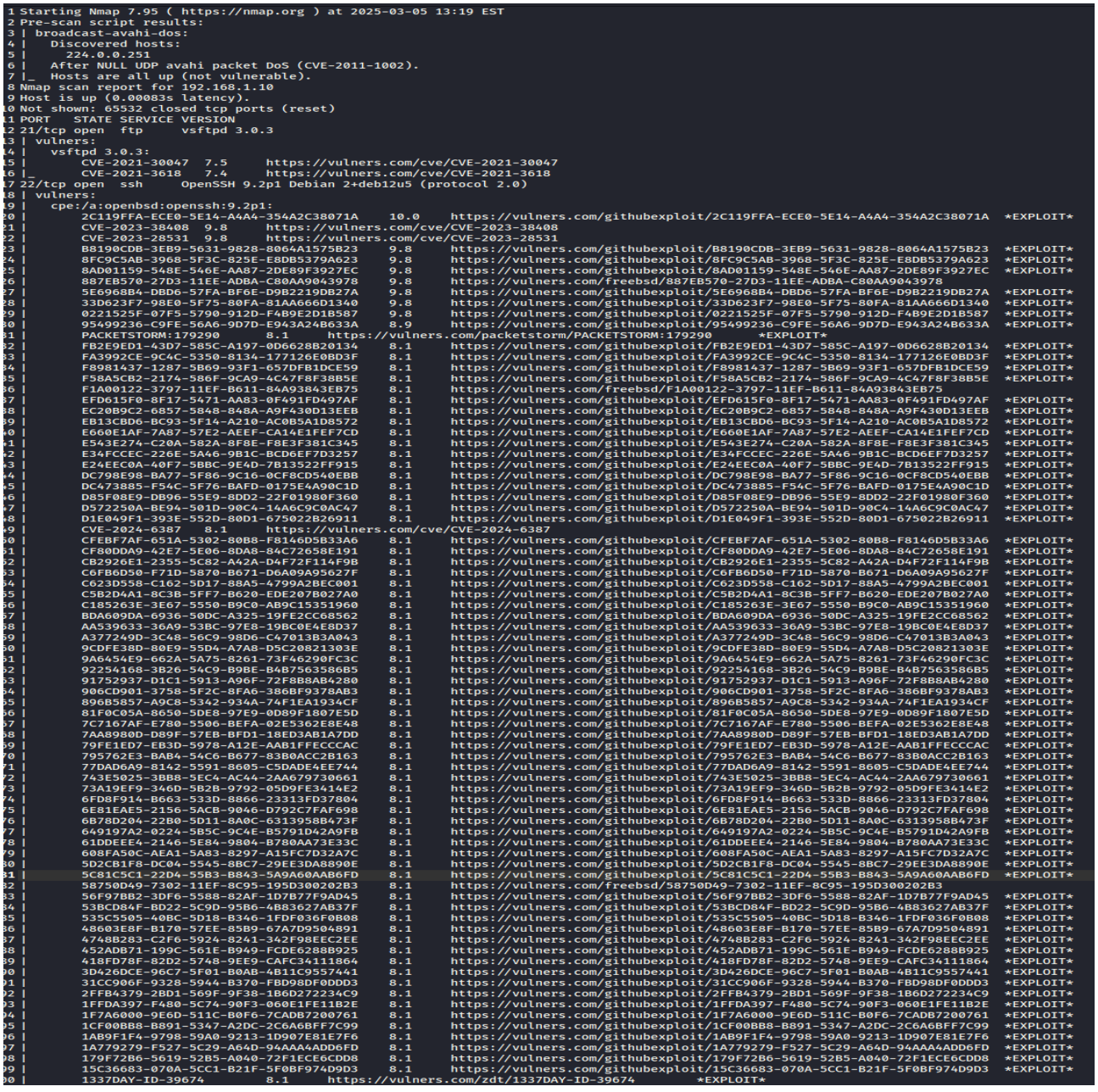
Vulnerabilities Report

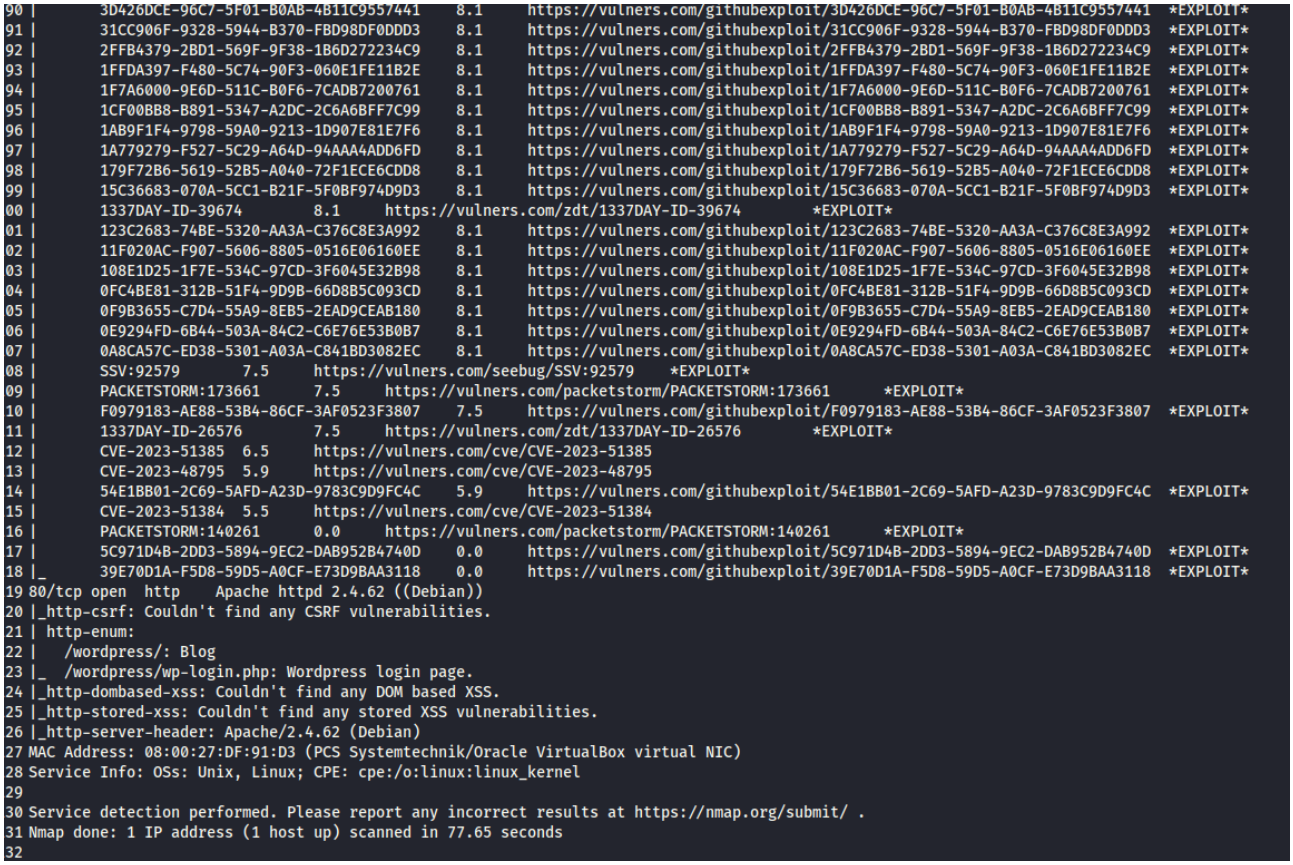
Verify the open ports and services running on the “Debian machine” with nmap command

Command used:

nmap -sV --script=vuln <debian_IP>

Results:





```
90 |       3D426DCE-96C7-5F01-B0AB-4B11C9557441    8.1     https://vulners.com/githubexploit/3D426DCE-96C7-5F01-B0AB-4B11C9557441  *EXPLOIT*
91 |       31CC906F-9328-5944-B370-FBD98DF0DDD3    8.1     https://vulners.com/githubexploit/31CC906F-9328-5944-B370-FBD98DF0DDD3  *EXPLOIT*
92 |       2FFB4379-2BD1-569F-9F38-1B6D272234C9    8.1     https://vulners.com/githubexploit/2FFB4379-2BD1-569F-9F38-1B6D272234C9  *EXPLOIT*
93 |       1FFDA397-F480-5C74-90F3-060E1FE11B2E    8.1     https://vulners.com/githubexploit/1FFDA397-F480-5C74-90F3-060E1FE11B2E  *EXPLOIT*
94 |       1F7A6000-9E6D-511C-B0F6-7CADB7200761    8.1     https://vulners.com/githubexploit/1F7A6000-9E6D-511C-B0F6-7CADB7200761  *EXPLOIT*
95 |       1CF00BB8-B891-5347-A2DC-2C6A6BFF7C99    8.1     https://vulners.com/githubexploit/1CF00BB8-B891-5347-A2DC-2C6A6BFF7C99  *EXPLOIT*
96 |       1AB9F1F4-9798-59A0-9213-1D907E81E7F6    8.1     https://vulners.com/githubexploit/1AB9F1F4-9798-59A0-9213-1D907E81E7F6  *EXPLOIT*
97 |       1A779279-F527-5C29-A64D-94AAA4ADD6FD    8.1     https://vulners.com/githubexploit/1A779279-F527-5C29-A64D-94AAA4ADD6FD  *EXPLOIT*
98 |       179F72B6-5619-52B5-A040-72F1ECE6CDD8    8.1     https://vulners.com/githubexploit/179F72B6-5619-52B5-A040-72F1ECE6CDD8  *EXPLOIT*
99 |       15C36683-070A-5CC1-B21F-5F0BF974D9D3    8.1     https://vulners.com/githubexploit/15C36683-070A-5CC1-B21F-5F0BF974D9D3  *EXPLOIT*
00 |       1337DAY-ID-39674        8.1     https://vulners.com/zdt/1337DAY-ID-39674        *EXPLOIT*
01 |       123C2683-74BE-5320-AA3A-C376C8E3A992    8.1     https://vulners.com/githubexploit/123C2683-74BE-5320-AA3A-C376C8E3A992  *EXPLOIT*
02 |       11F020AC-F907-5606-8805-0516E06160EE    8.1     https://vulners.com/githubexploit/11F020AC-F907-5606-8805-0516E06160EE  *EXPLOIT*
03 |       108E1D25-1F7E-534C-97CD-3F6045E32B98    8.1     https://vulners.com/githubexploit/108E1D25-1F7E-534C-97CD-3F6045E32B98  *EXPLOIT*
04 |       0FC4BE81-312B-51F4-9D9B-66D8B5C093CD    8.1     https://vulners.com/githubexploit/0FC4BE81-312B-51F4-9D9B-66D8B5C093CD  *EXPLOIT*
05 |       0F9B3655-C7D4-55A9-8EB5-2EAD9CEAB180    8.1     https://vulners.com/githubexploit/0F9B3655-C7D4-55A9-8EB5-2EAD9CEAB180  *EXPLOIT*
06 |       0E9294FD-6B44-503A-84C2-C6E76E53B0B7    8.1     https://vulners.com/githubexploit/0E9294FD-6B44-503A-84C2-C6E76E53B0B7  *EXPLOIT*
07 |       0A8CA57C-ED38-5301-A03A-C841BD3082EC    8.1     https://vulners.com/githubexploit/0A8CA57C-ED38-5301-A03A-C841BD3082EC  *EXPLOIT*
08 |       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *EXPLOIT*
09 |       PACKETSTORM:173661      7.5     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
10 |       F0979183-AE88-53B4-86CF-3AF0523F3807    7.5     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807  *EXPLOIT*
11 |       1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-26576        *EXPLOIT*
12 |       CVE-2023-51385  6.5     https://vulners.com/cve/CVE-2023-51385
13 |       CVE-2023-48795  5.9     https://vulners.com/cve/CVE-2023-48795
14 |       54E1BB01-2C69-5AFD-A23D-9783C9D9FC4C    5.9     https://vulners.com/githubexploit/54E1BB01-2C69-5AFD-A23D-9783C9D9FC4C  *EXPLOIT*
15 |       CVE-2023-51384  5.5     https://vulners.com/cve/CVE-2023-51384
16 |       PACKETSTORM:140261      0.0     https://vulners.com/packetstorm/PACKETSTORM:140261      *EXPLOIT*
17 |       5C971D4B-2DD3-5894-9EC2-DAB952B4740D    0.0     https://vulners.com/githubexploit/5C971D4B-2DD3-5894-9EC2-DAB952B4740D  *EXPLOIT*
18 |_      39E70D1A-F5D8-59D5-A0CF-E73D9BAA3118    0.0     https://vulners.com/githubexploit/39E70D1A-F5D8-59D5-A0CF-E73D9BAA3118  *EXPLOIT*
19 80/tcp open  http    Apache httpd 2.4.62 ((Debian))
20 |_http-csrf: Couldn't find any CSRF vulnerabilities.
21 | http-enum:
22 |   /wordpress/: Blog
23 |_  /wordpress/wp-login.php: Wordpress login page.
24 |_http-dombased-xss: Couldn't find any DOM based XSS.
25 |_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
26 |_http-server-header: Apache/2.4.62 (Debian)
27 MAC Address: 08:00:27:DF:91:D3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
28 Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
29
30 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
31 Nmap done: 1 IP address (1 host up) scanned in 77.65 seconds
32
```

vulnerabilities found:

Port	Service	Version	Vulnerability	Description	Reference
21	FTP	Vsftpd 3.0.3	CVE-2021-30047	VSFTPD 3.0.3 allows attackers to cause a denial of service due to limited number of connections allowed.	https://nvd.nist.gov/vuln/detail/CVE-2021-30047
22	SSH	OpenSSH 9.2p1	CVE-2023-38408	Feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system	https://nvd.nist.gov/vuln/detail/CVE-2023-38408

Port “80/tcp open http Apache httpd 2.4.62” the nmap command find that is open but cannot find any vulnerability that does not mean that it does not have it, could have some vulnerabilities that are not founded here , should be investigated in depth using more tools to find attacks against Apache and Wordpress.