Vulnerabilidades Debian

Listado extraído de NMAP

```
┌──(root㉿kali)-[/home/kali/repo/scan-with-nmap-practiceCCT]
└─# nmap -sV 192.168.1.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 15:01 EDT
Nmap scan report for 192.168.1.140
Host is up (0.00063s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:D1:65:C7 (Oracle VirtualBox virtual NIC)
Service Info: OS: 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 7.27 seconds

┌──(root㉿kali)-[/home/kali/repo/scan-with-nmap-practiceCCT]
└─# nmap -sV --script=vuln 192.168.1.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 15:01 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 192.168.1.140
Host is up (0.0010s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:9.2p1:
|       95499236-C9FE-56A6-9D7D-E943A24B633A    10.0
https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A
*EXPLOIT*
|       2C119FFA-ECE0-5E14-A4A4-354A2C38071A    10.0
https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A
*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/B8190CDB-3EB9-5631-9828-8064A1575B23
*EXPLOIT*
|	8FC9C5AB-3968-5F3C-825E-E8DB5379A623	9.8
https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623
*EXPLOIT*
|	8AD01159-548E-546E-AA87-2DE89F3927EC	9.8
https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC
*EXPLOIT*
|	5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A	9.8
https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A
*EXPLOIT*
|	33D623F7-98E0-5F75-80FA-81AA666D1340	9.8
https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340
*EXPLOIT*
|	PACKETSTORM:179290	8.1
https://vulners.com/packetstorm/PACKETSTORM:179290	*EXPLOIT*
|	FB2E9ED1-43D7-585C-A197-0D6628B20134	8.1
https://vulners.com/githubexploit/FB2E9ED1-43D7-585C-A197-0D6628B20134
*EXPLOIT*
|	FA3992CE-9C4C-5350-8134-177126E0BD3F	8.1
https://vulners.com/githubexploit/FA3992CE-9C4C-5350-8134-177126E0BD3F
*EXPLOIT*
|	F8981437-1287-5B69-93F1-657DFB1DCE59	8.1
https://vulners.com/githubexploit/F8981437-1287-5B69-93F1-657DFB1DCE59
*EXPLOIT*
|	F58A5CB2-2174-586F-9CA9-4C47F8F38B5E	8.1
https://vulners.com/githubexploit/F58A5CB2-2174-586F-9CA9-4C47F8F38B5E
*EXPLOIT*
|	EFD615F0-8F17-5471-AA83-0F491FD497AF	8.1
https://vulners.com/githubexploit/EFD615F0-8F17-5471-AA83-0F491FD497AF
*EXPLOIT*
|	EC20B9C2-6857-5848-848A-A9F430D13EEB	8.1
https://vulners.com/githubexploit/EC20B9C2-6857-5848-848A-A9F430D13EEB
*EXPLOIT*
|	EB13CBD6-BC93-5F14-A210-AC0B5A1D8572	8.1
https://vulners.com/githubexploit/EB13CBD6-BC93-5F14-A210-AC0B5A1D8572
*EXPLOIT*
|	E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD	8.1
https://vulners.com/githubexploit/E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD
*EXPLOIT*
|	E543E274-C20A-582A-8F8E-F8E3F381C345	8.1
https://vulners.com/githubexploit/E543E274-C20A-582A-8F8E-F8E3F381C345
*EXPLOIT*
|	E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257	8.1
https://vulners.com/githubexploit/E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257
*EXPLOIT*
```

```
|       E24EEC0A-40F7-5BBC-9E4D-7B13522FF915    8.1
https://vulners.com/githubexploit/E24EEC0A-40F7-5BBC-9E4D-7B13522FF915
*EXPLOIT*
|       DC798E98-BA77-5F86-9C16-0CF8CD540EBB    8.1
https://vulners.com/githubexploit/DC798E98-BA77-5F86-9C16-0CF8CD540EBB
*EXPLOIT*
|       DC473885-F54C-5F76-BAFD-0175E4A90C1D    8.1
https://vulners.com/githubexploit/DC473885-F54C-5F76-BAFD-0175E4A90C1D
*EXPLOIT*
|       D85F08E9-DB96-55E9-8DD2-22F01980F360    8.1
https://vulners.com/githubexploit/D85F08E9-DB96-55E9-8DD2-22F01980F360
*EXPLOIT*
|       D572250A-BE94-501D-90C4-14A6C9C0AC47    8.1
https://vulners.com/githubexploit/D572250A-BE94-501D-90C4-14A6C9C0AC47
*EXPLOIT*
|       D1E049F1-393E-552D-80D1-675022B26911    8.1
https://vulners.com/githubexploit/D1E049F1-393E-552D-80D1-675022B26911
*EXPLOIT*
|       CVE-2024-6387   8.1     https://vulners.com/cve/CVE-2024-6387
|       CFEBF7AF-651A-5302-80B8-F8146D5B33A6    8.1
https://vulners.com/githubexploit/CFEBF7AF-651A-5302-80B8-F8146D5B33A6
*EXPLOIT*
|       CF80DDA9-42E7-5E06-8DA8-84C72658E191    8.1
https://vulners.com/githubexploit/CF80DDA9-42E7-5E06-8DA8-84C72658E191
*EXPLOIT*
|       CB2926E1-2355-5C82-A42A-D4F72F114F9B    8.1
https://vulners.com/githubexploit/CB2926E1-2355-5C82-A42A-D4F72F114F9B
*EXPLOIT*
|       C6FB6D50-F71D-5870-B671-D6A09A95627F    8.1
https://vulners.com/githubexploit/C6FB6D50-F71D-5870-B671-D6A09A95627F
*EXPLOIT*
|       C5B2D4A1-8C3B-5FF7-B620-EDE207B027A0    8.1
https://vulners.com/githubexploit/C5B2D4A1-8C3B-5FF7-B620-EDE207B027A0
*EXPLOIT*
|       C185263E-3E67-5550-B9C0-AB9C15351960    8.1
https://vulners.com/githubexploit/C185263E-3E67-5550-B9C0-AB9C15351960
*EXPLOIT*
|       BDA609DA-6936-50DC-A325-19FE2CC68562    8.1
https://vulners.com/githubexploit/BDA609DA-6936-50DC-A325-19FE2CC68562
*EXPLOIT*
|       AA539633-36A9-53BC-97E8-19BC0E4E8D37    8.1
https://vulners.com/githubexploit/AA539633-36A9-53BC-97E8-19BC0E4E8D37
*EXPLOIT*
|       A377249D-3C48-56C9-98D6-C47013B3A043    8.1
https://vulners.com/githubexploit/A377249D-3C48-56C9-98D6-C47013B3A043
*EXPLOIT*
```

```
|       9CDFE38D-80E9-55D4-A7A8-D5C20821303E    8.1
https://vulners.com/githubexploit/9CDFE38D-80E9-55D4-A7A8-D5C20821303E
*EXPLOIT*
|       9A6454E9-662A-5A75-8261-73F46290FC3C    8.1
https://vulners.com/githubexploit/9A6454E9-662A-5A75-8261-73F46290FC3C
*EXPLOIT*
|       92254168-3B26-54C9-B9BE-B4B7563586B5    8.1
https://vulners.com/githubexploit/92254168-3B26-54C9-B9BE-B4B7563586B5
*EXPLOIT*
|       91752937-D1C1-5913-A96F-72F8B8AB4280    8.1
https://vulners.com/githubexploit/91752937-D1C1-5913-A96F-72F8B8AB4280
*EXPLOIT*
|       906CD901-3758-5F2C-8FA6-386BF9378AB3    8.1
https://vulners.com/githubexploit/906CD901-3758-5F2C-8FA6-386BF9378AB3
*EXPLOIT*
|       896B5857-A9C8-5342-934A-74F1EA1934CF    8.1
https://vulners.com/githubexploit/896B5857-A9C8-5342-934A-74F1EA1934CF
*EXPLOIT*
|       81F0C05A-8650-5DE8-97E9-0D89F1807E5D    8.1
https://vulners.com/githubexploit/81F0C05A-8650-5DE8-97E9-0D89F1807E5D
*EXPLOIT*
|       7C7167AF-E780-5506-BEFA-02E5362E8E48    8.1
https://vulners.com/githubexploit/7C7167AF-E780-5506-BEFA-02E5362E8E48
*EXPLOIT*
|       7AA8980D-D89F-57EB-BFD1-18ED3AB1A7DD    8.1
https://vulners.com/githubexploit/7AA8980D-D89F-57EB-BFD1-18ED3AB1A7DD
*EXPLOIT*
|       79FE1ED7-EB3D-5978-A12E-AAB1FFECCCAC    8.1
https://vulners.com/githubexploit/79FE1ED7-EB3D-5978-A12E-AAB1FFECCCAC
*EXPLOIT*
|       795762E3-BAB4-54C6-B677-83B0ACC2B163    8.1
https://vulners.com/githubexploit/795762E3-BAB4-54C6-B677-83B0ACC2B163
*EXPLOIT*
|       77DAD6A9-8142-5591-8605-C5DADE4EE744    8.1
https://vulners.com/githubexploit/77DAD6A9-8142-5591-8605-C5DADE4EE744
*EXPLOIT*
|       743E5025-3BB8-5EC4-AC44-2AA679730661    8.1
https://vulners.com/githubexploit/743E5025-3BB8-5EC4-AC44-2AA679730661
*EXPLOIT*
|       73A19EF9-346D-5B2B-9792-05D9FE3414E2    8.1
https://vulners.com/githubexploit/73A19EF9-346D-5B2B-9792-05D9FE3414E2
*EXPLOIT*
|       6FD8F914-B663-533D-8866-23313FD37804    8.1
https://vulners.com/githubexploit/6FD8F914-B663-533D-8866-23313FD37804
*EXPLOIT*
```

```
|	6E81EAE5-2156-5ACB-9046-D792C7FAF698	8.1
https://vulners.com/githubexploit/6E81EAE5-2156-5ACB-9046-D792C7FAF698
*EXPLOIT*
|	6B78D204-22B0-5D11-8A0C-6313958B473F	8.1
https://vulners.com/githubexploit/6B78D204-22B0-5D11-8A0C-6313958B473F
*EXPLOIT*
|	649197A2-0224-5B5C-9C4E-B5791D42A9FB	8.1
https://vulners.com/githubexploit/649197A2-0224-5B5C-9C4E-B5791D42A9FB
*EXPLOIT*
|	608FA50C-AEA1-5A83-8297-A15FC7D32A7C	8.1
https://vulners.com/githubexploit/608FA50C-AEA1-5A83-8297-A15FC7D32A7C
*EXPLOIT*
|	5D2CB1F8-DC04-5545-8BC7-29EE3DA8890E	8.1
https://vulners.com/githubexploit/5D2CB1F8-DC04-5545-8BC7-29EE3DA8890E
*EXPLOIT*
|	5C81C5C1-22D4-55B3-B843-5A9A60AAB6FD	8.1
https://vulners.com/githubexploit/5C81C5C1-22D4-55B3-B843-5A9A60AAB6FD
*EXPLOIT*
|	56F97BB2-3DF6-5588-82AF-1D7B77F9AD45	8.1
https://vulners.com/githubexploit/56F97BB2-3DF6-5588-82AF-1D7B77F9AD45
*EXPLOIT*
|	53BCD84F-BD22-5C9D-95B6-4B83627AB37F	8.1
https://vulners.com/githubexploit/53BCD84F-BD22-5C9D-95B6-4B83627AB37F
*EXPLOIT*
|	535C5505-40BC-5D18-B346-1FDF036F0B08	8.1
https://vulners.com/githubexploit/535C5505-40BC-5D18-B346-1FDF036F0B08
*EXPLOIT*
|	48603E8F-B170-57EE-85B9-67A7D9504891	8.1
https://vulners.com/githubexploit/48603E8F-B170-57EE-85B9-67A7D9504891
*EXPLOIT*
|	4748B283-C2F6-5924-8241-342F98EEC2EE	8.1
https://vulners.com/githubexploit/4748B283-C2F6-5924-8241-342F98EEC2EE
*EXPLOIT*
|	452ADB71-199C-561E-B949-FCDE6288B925	8.1
https://vulners.com/githubexploit/452ADB71-199C-561E-B949-FCDE6288B925
*EXPLOIT*
|	418FD78F-82D2-5748-9EE9-CAFC34111864	8.1
https://vulners.com/githubexploit/418FD78F-82D2-5748-9EE9-CAFC34111864
*EXPLOIT*
|	3D426DCE-96C7-5F01-B0AB-4B11C9557441	8.1
https://vulners.com/githubexploit/3D426DCE-96C7-5F01-B0AB-4B11C9557441
*EXPLOIT*
|	31CC906F-9328-5944-B370-FBD98DF0DDD3	8.1
https://vulners.com/githubexploit/31CC906F-9328-5944-B370-FBD98DF0DDD3
*EXPLOIT*
```

```
|       2FFB4379-2BD1-569F-9F38-1B6D272234C9    8.1
https://vulners.com/githubexploit/2FFB4379-2BD1-569F-9F38-1B6D272234C9
*EXPLOIT*
|       1FFDA397-F480-5C74-90F3-060E1FE11B2E    8.1
https://vulners.com/githubexploit/1FFDA397-F480-5C74-90F3-060E1FE11B2E
*EXPLOIT*
|       1F7A6000-9E6D-511C-B0F6-7CADB7200761    8.1
https://vulners.com/githubexploit/1F7A6000-9E6D-511C-B0F6-7CADB7200761
*EXPLOIT*
|       1CF00BB8-B891-5347-A2DC-2C6A6BFF7C99    8.1
https://vulners.com/githubexploit/1CF00BB8-B891-5347-A2DC-2C6A6BFF7C99
*EXPLOIT*
|       1AB9F1F4-9798-59A0-9213-1D907E81E7F6    8.1
https://vulners.com/githubexploit/1AB9F1F4-9798-59A0-9213-1D907E81E7F6
*EXPLOIT*
|       1A779279-F527-5C29-A64D-94AAA4ADD6FD    8.1
https://vulners.com/githubexploit/1A779279-F527-5C29-A64D-94AAA4ADD6FD
*EXPLOIT*
|       15C36683-070A-5CC1-B21F-5F0BF974D9D3    8.1
https://vulners.com/githubexploit/15C36683-070A-5CC1-B21F-5F0BF974D9D3
*EXPLOIT*
|       1337DAY-ID-39674        8.1     https://vulners.com/zdt/1337DAY-ID-39674
*EXPLOIT*
|       11F020AC-F907-5606-8805-0516E06160EE    8.1
https://vulners.com/githubexploit/11F020AC-F907-5606-8805-0516E06160EE
*EXPLOIT*
|       108E1D25-1F7E-534C-97CD-3F6045E32B98    8.1
https://vulners.com/githubexploit/108E1D25-1F7E-534C-97CD-3F6045E32B98
*EXPLOIT*
|       0FC4BE81-312B-51F4-9D9B-66D8B5C093CD    8.1
https://vulners.com/githubexploit/0FC4BE81-312B-51F4-9D9B-66D8B5C093CD
*EXPLOIT*
|       0F9B3655-C7D4-55A9-8EB5-2EAD9CEAB180    8.1
https://vulners.com/githubexploit/0F9B3655-C7D4-55A9-8EB5-2EAD9CEAB180
*EXPLOIT*
|       0E9294FD-6B44-503A-84C2-C6E76E53B0B7    8.1
https://vulners.com/githubexploit/0E9294FD-6B44-503A-84C2-C6E76E53B0B7
*EXPLOIT*
|       0A8CA57C-ED38-5301-A03A-C841BD3082EC    8.1
https://vulners.com/githubexploit/0A8CA57C-ED38-5301-A03A-C841BD3082EC
*EXPLOIT*
|       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *EXPLOIT*
|       PACKETSTORM:173661      7.5
https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    7.5
https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807
*EXPLOIT*
```

```
|       1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-26576
*EXPLOIT*
|       CVE-2023-51385  6.5     https://vulners.com/cve/CVE-2023-51385
|       CVE-2023-48795  5.9     https://vulners.com/cve/CVE-2023-48795
|       CVE-2023-51384  5.5     https://vulners.com/cve/CVE-2023-51384
|       PACKETSTORM:140261      0.0
https://vulners.com/packetstorm/PACKETSTORM:140261      *EXPLOIT*
|       5C971D4B-2DD3-5894-9EC2-DAB952B4740D    0.0
https://vulners.com/githubexploit/5C971D4B-2DD3-5894-9EC2-DAB952B4740D
*EXPLOIT*
|_      39E70D1A-F5D8-59D5-A0CF-E73D9BAA3118    0.0
https://vulners.com/githubexploit/39E70D1A-F5D8-59D5-A0CF-E73D9BAA3118
*EXPLOIT*
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_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-enum:
|   /wordpress/: Blog
|   /phpmyadmin/: phpMyAdmin
|_  /wordpress/wp-login.php: Wordpress login page.
MAC Address: 08:00:27:D1:65:C7 (Oracle VirtualBox virtual NIC)
Service Info: OS: 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 64.13 seconds
```

OPEN SSH   OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)

⍰ **CVE-2023-25136**: This pre-authentication double-free vulnerability allows potential remote code execution (RCE) or denial-of-service (DoS) attacks. It exploits a memory management error in handling SSH key exchange algorithms, but due to the security mechanisms like sandboxing and privilege separation in OpenSSH, the exploit is difficult to achieve. It mostly impacts versions before 9.2p1.

⍰ **CVE-2024-6387 ("regreSSHion")**: A newly discovered remote code execution flaw allows unauthenticated attackers to gain root privileges on Linux systems. This vulnerability exploits a race condition in the SSH daemon's signal handling. While challenging to exploit, this vulnerability could lead to full system compromise

80/tcp open http   Apache httpd 2.4.62 ((Debian))

⍰ **CVE-2024-40725 & CVE-2024-40898**: These vulnerabilities could allow HTTP request smuggling and SSL client authentication bypass, potentially leading to unauthorized access or further attacks like session hijacking or command injection

Censys

.

⍰ **CVE-2024-39884**: A regression in version 2.4.60 could expose local content (e.g., PHP scripts) instead of processing them, leading to source code disclosure

Debian Security Tracker

.

⍰ **CVE-2024-38476**: A flaw in earlier versions could expose Apache HTTP Server to SSRF (Server-Side Request Forgery) and local script execution due to malicious response headers