Informe de Vulnerabilidades

Información General del Host

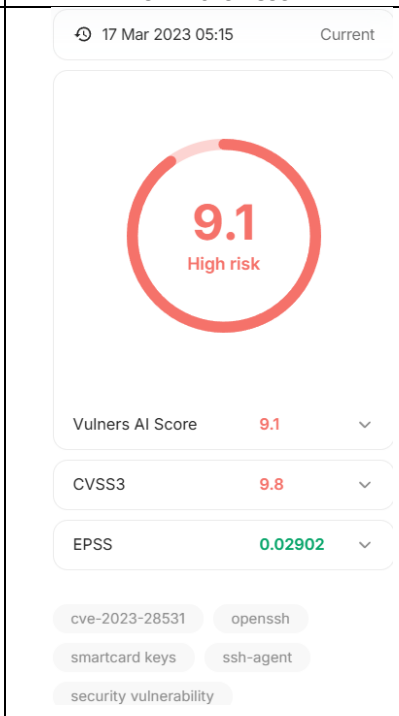
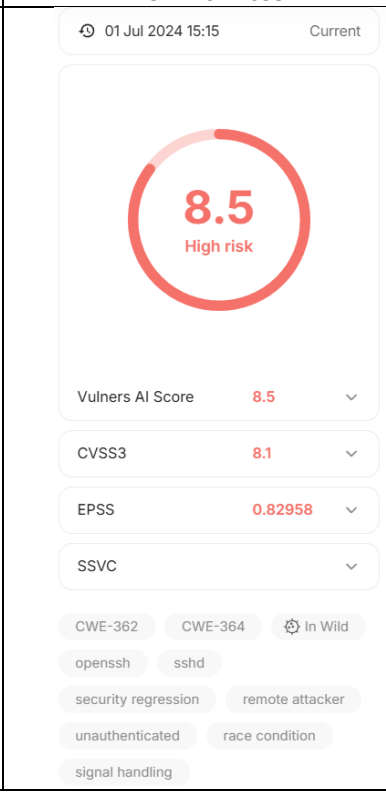
IP	192.168.100.221
Sistema Operativo	Linux
MAC Address	08:00:27:D1:65:C7 (Oracle VirtualBox virtual NIC)
SSH	OpenSSH 9.2p1 Debian 2+deb12u5 (protocolo 2.0)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.100.221
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 23:16 EDT
Nmap scan report for 192.168.100.221
Host is up (0.00023s latency).
Not shown: 979 filtered tcp ports (no-response), 20 filtered tcp ports (admin-prohibited)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/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 14.63 seconds
```

Detalle de Vulnerabilidades Identificadas

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script=vuln 192.168.100.221
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 23:22 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 192.168.100.221
Host is up (0.00023s latency).
Not shown: 980 filtered tcp ports (no-response), 19 filtered tcp ports (admin-prohibited)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:9.2p1:
|       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*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587  *EXPLOIT*
|       95499236-C9FE-56A6-9D7D-E943A24B633A    8.9     https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A  *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*
|       C623D558-C162-5D17-88A5-4799A2BEC001    8.1     https://vulners.com/githubexploit/C623D558-C162-5D17-88A5-4799A2BEC001  *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*
|       179F72B6-5619-52B5-A040-72F1ECE6CDD8    8.1     https://vulners.com/githubexploit/179F72B6-5619-52B5-A040-72F1ECE6CDD8  *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*
|       123C2683-74BE-5320-AA3A-C376C8E3A992    8.1     https://vulners.com/githubexploit/123C2683-74BE-5320-AA3A-C376C8E3A992  *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*
|       PACKETSTORM:189283      6.8     https://vulners.com/packetstorm/PACKETSTORM:189283      *EXPLOIT*
|       F79E574D-30C8-5C52-A801-66FFA0610BAA    6.8     https://vulners.com/githubexploit/F79E574D-30C8-5C52-A801-66FFA0610BAA  *EXPLOIT*
|       CVE-2025-26465  6.8     https://vulners.com/cve/CVE-2025-26465
|       1337DAY-ID-39918        6.8     https://vulners.com/zdt/1337DAY-ID-39918        *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
|       54E1BB01-2C69-5AFD-A23D-9783C9D9FC4C    5.9     https://vulners.com/githubexploit/54E1BB01-2C69-5AFD-A23D-9783C9D9FC4C  *EXPLOIT*
|       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*
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/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 49.22 seconds
```

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia link
22	SSH	OpenSSH 9.2p1 Debian 2+deb12u5	CVE-2023-38408	Ejecución remota de código	CVE-2023-38408
22	SSH	OpenSSH 9.2p1 Debian 2+deb12u5	CVE-2023-28531	Vulnerabilidad de autenticación	CVE-2023-28531
22	SSH	Open SSH 9.2p1 Debian 2+deb12u5	CVE-2024-6387	Escalamiento de privilegios	CVE-2024-6387

CVE-2023-38408	CVE-2023-28531	CVE-2024-6387
		

Recomendaciones

1. Actualizar OpenSSH, se recomienda actualizar a la última versión disponible para mitigar los riesgos.
2. Restringir Acceso, configurar firewalls y políticas de acceso para minimizar la exposición del servicio SSH.
3. Auditoría de Seguridad, realizar auditorías regulares para detectar nuevas vulnerabilidades.
4. Parcheo de Seguridad, aplicar parches de seguridad recomendados por los desarrolladores del sistema operativo.