Raven

Walk

Primero buscar el host

```
┌──(kali㉿kali)-[~/Desktop/Raven]
└─$ nmap 66.66.66.0/24
```

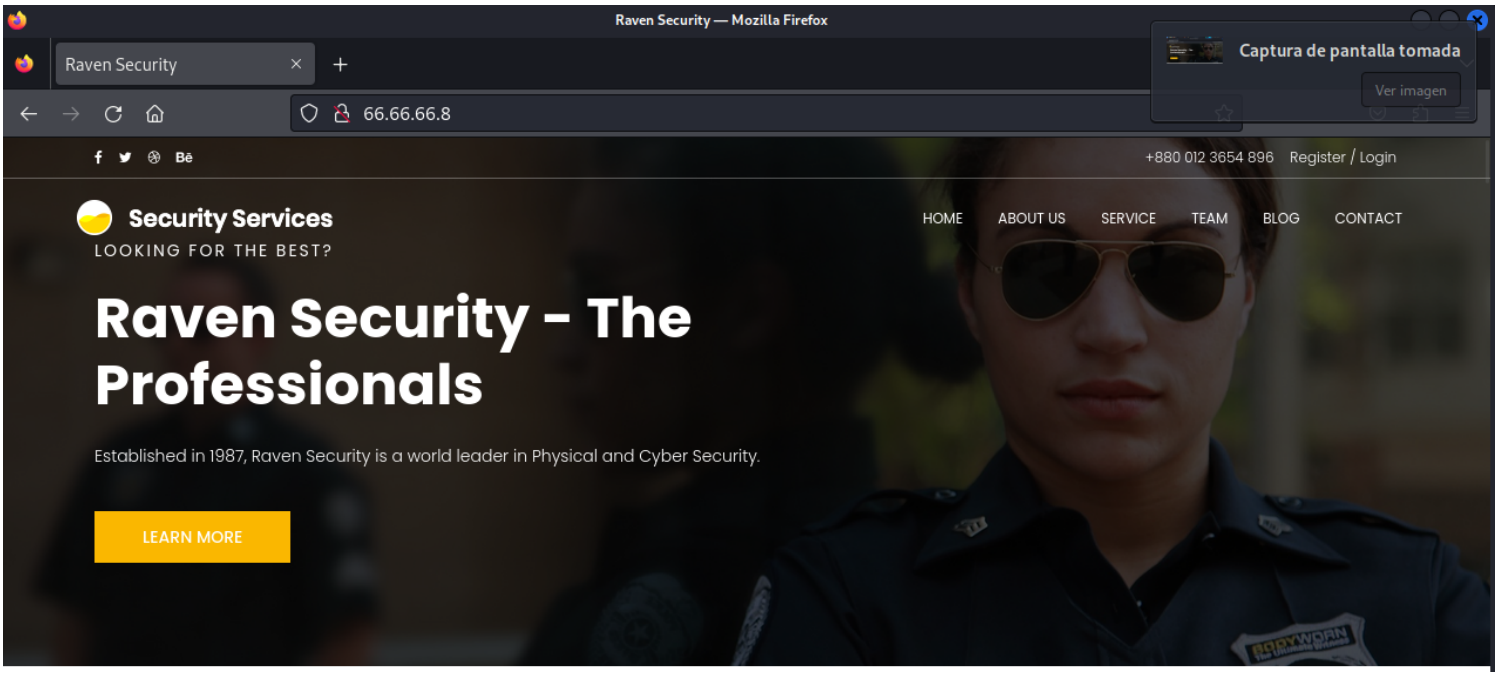
```
Nmap scan report for 066-066-066-008.res.spectrum.com (66.66.66.8)
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind

Nmap done: 256 IP addresses (3 hosts up) scanned in 4.34 seconds
IP : 66.66.66.8
```

comenzamos a escanear

```
┌──(kali㉿kali)-[~/Desktop/Raven]
└─$ $ sudo nmap -sS -sV --script vuln auth default 66.66.66.8 -v -oA raven
```

Ingresamos al puerto 80 ,



Seg`un el escaneo , esta p`agina es un wordpress
lo que hare es enumerar las paginas y directorios

```
┌──(kali㉿kali)-[~/Desktop/Raven]
└─$  nikto -h 66.66.66.8 -o nikto_raven.txt
```

es hora de escanear el wordpress para ver que pasa

```
 wpscan --url http://66.66.66.8/wordpress –enumerate vp,vt,u
```

Escaneo

```
└─$ sudo nmap -sS -sV --script vuln auth default 66.66.66.8 -v -oA raven
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-13 11:27 EST
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:27
Completed NSE at 11:27, 10.02s elapsed
Initiating NSE at 11:27
Completed NSE at 11:27, 0.00s elapsed
Failed to resolve "auth".
Failed to resolve "default".
Initiating ARP Ping Scan at 11:27
Scanning 66.66.66.8 [1 port]
Completed ARP Ping Scan at 11:27, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:27
Completed Parallel DNS resolution of 1 host. at 11:27, 0.01s elapsed
Initiating SYN Stealth Scan at 11:27
Scanning 066-066-066-008.res.spectrum.com (66.66.66.8) [1000 ports]
Discovered open port 80/tcp on 66.66.66.8
Discovered open port 22/tcp on 66.66.66.8
Discovered open port 111/tcp on 66.66.66.8
Completed SYN Stealth Scan at 11:27, 0.15s elapsed (1000 total ports)
Initiating Service scan at 11:27
Scanning 3 services on 066-066-066-008.res.spectrum.com (66.66.66.8)
Completed Service scan at 11:27, 6.07s elapsed (3 services on 1 host)
NSE: Script scanning 66.66.66.8.
Initiating NSE at 11:27
Completed NSE at 11:27, 23.12s elapsed
Initiating NSE at 11:27
Completed NSE at 11:27, 0.07s elapsed
Nmap scan report for 066-066-066-008.res.spectrum.com (66.66.66.8)
Host is up (0.0020s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
|       PRION:CVE-2015-5600     8.5     https://vulners.com/prion/PRION:CVE-2015-5600
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       PRION:CVE-2020-16088    7.5     https://vulners.com/prion/PRION:CVE-2020-16088
|       PRION:CVE-2015-6564     6.9     https://vulners.com/prion/PRION:CVE-2015-6564
|       CVE-2015-6564   6.9     https://vulners.com/cve/CVE-2015-6564
|       CVE-2018-15919  5.0     https://vulners.com/cve/CVE-2018-15919
|       SSV:90447       4.6     https://vulners.com/seebug/SSV:90447    *EXPLOIT*
|       PRION:CVE-2016-0778     4.6     https://vulners.com/prion/PRION:CVE-2016-0778
|       CVE-2016-0778   4.6     https://vulners.com/cve/CVE-2016-0778
|       PRION:CVE-2015-5352     4.3     https://vulners.com/prion/PRION:CVE-2015-5352
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2015-5352   4.3     https://vulners.com/cve/CVE-2015-5352
|       PRION:CVE-2016-0777     4.0     https://vulners.com/prion/PRION:CVE-2016-0777
|       CVE-2016-0777   4.0     https://vulners.com/cve/CVE-2016-0777
|       PRION:CVE-2015-6563     1.9     https://vulners.com/prion/PRION:CVE-2015-6563
|_      CVE-2015-6563   1.9     https://vulners.com/cve/CVE-2015-6563
80/tcp  open  http    Apache httpd 2.4.10 ((Debian))
| vulners:
|   cpe:/a:apache:http_server:2.4.10:
|       PACKETSTORM:171631      7.5     https://vulners.com/packetstorm/PACKETSTORM:171631      *EXPLOIT*
|       EDB-ID:51193    7.5     https://vulners.com/exploitdb/EDB-ID:51193      *EXPLOIT*
|       CVE-2022-31813  7.5     https://vulners.com/cve/CVE-2022-31813
```

| CVE-2022-23943 7.5 https://vulners.com/cve/CVE-2022-23943
| CVE-2022-22720 7.5 https://vulners.com/cve/CVE-2022-22720
| CVE-2021-44790 7.5 https://vulners.com/cve/CVE-2021-44790
| CVE-2021-39275 7.5 https://vulners.com/cve/CVE-2021-39275
| CVE-2021-26691 7.5 https://vulners.com/cve/CVE-2021-26691
| CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679
| CVE-2017-3169 7.5 https://vulners.com/cve/CVE-2017-3169
| CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167
| CNVD-2022-73123 7.5 https://vulners.com/cnvd/CNVD-2022-73123
| CNVD-2022-03225 7.5 https://vulners.com/cnvd/CNVD-2022-03225
| CNVD-2021-102386 7.5 https://vulners.com/cnvd/CNVD-2021-102386
| 1337DAY-ID-38427 7.5 https://vulners.com/zdt/1337DAY-ID-38427 *EXPLOIT*
| FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 6.8 https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 *EXPLOIT*
| CVE-2021-40438 6.8 https://vulners.com/cve/CVE-2021-40438
| CVE-2020-35452 6.8 https://vulners.com/cve/CVE-2020-35452
| CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312
| CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715
| CVE-2016-5387 6.8 https://vulners.com/cve/CVE-2016-5387
| CVE-2014-0226 6.8 https://vulners.com/cve/CVE-2014-0226
| CNVD-2022-03224 6.8 https://vulners.com/cnvd/CNVD-2022-03224
| AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C 6.8 https://vulners.com/githubexploit/AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C *EXPLOIT*
| 8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 6.8 https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 *EXPLOIT*
| 4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 6.8 https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 *EXPLOIT*
| 4373C92A-2755-5538-9C91-0469C995AA9B 6.8 https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B *EXPLOIT*
| 36618CA8-9316-59CA-B748-82F15F407C4F 6.8 https://vulners.com/githubexploit/36618CA8-9316-59CA-B748-82F15F407C4F *EXPLOIT*
| 0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8 https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE *EXPLOIT*
| OSV:BIT-2023-31122 6.4 https://vulners.com/osv/OSV:BIT-2023-31122
| CVE-2022-28615 6.4 https://vulners.com/cve/CVE-2022-28615
| CVE-2021-44224 6.4 https://vulners.com/cve/CVE-2021-44224
| CVE-2017-9788 6.4 https://vulners.com/cve/CVE-2017-9788
| CVE-2019-0217 6.0 https://vulners.com/cve/CVE-2019-0217
| CVE-2022-22721 5.8 https://vulners.com/cve/CVE-2022-22721
| CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927
| CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098
| 1337DAY-ID-33577 5.8 https://vulners.com/zdt/1337DAY-ID-33577 *EXPLOIT*
| CVE-2022-36760 5.1 https://vulners.com/cve/CVE-2022-36760
| SSV:96537 5.0 https://vulners.com/seebug/SSV:96537 *EXPLOIT*
| SSV:62058 5.0 https://vulners.com/seebug/SSV:62058 *EXPLOIT*
| OSV:BIT-2023-45802 5.0 https://vulners.com/osv/OSV:BIT-2023-45802
| OSV:BIT-2023-43622 5.0 https://vulners.com/osv/OSV:BIT-2023-43622
| F7F6E599-CEF4-5E03-8E10-FE18C4101E38 5.0 https://vulners.com/githubexploit/F7F6E599-CEF4-5E03-8E10-FE18C4101E38 *EXPLOIT*
| EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7 5.0 https://vulners.com/exploitpack/EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7 *EXPLOIT*
| EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D 5.0 https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D *EXPLOIT*
| EDB-ID:42745 5.0 https://vulners.com/exploitdb/EDB-ID:42745 *EXPLOIT*
| EDB-ID:40961 5.0 https://vulners.com/exploitdb/EDB-ID:40961 *EXPLOIT*
| E5C174E5-D6E8-56E0-8403-D287DE52EB3F 5.0 https://vulners.com/githubexploit/E5C174E5-D6E8-56E0-8403-D287DE52EB3F *EXPLOIT*
| DB6E1BBD-08B1-574D-A351-7D6BB9898A4A 5.0 https://vulners.com/githubexploit/DB6E1BBD-08B1-574D-A351-7D6BB9898A4A *EXPLOIT*
| CVE-2022-37436 5.0 https://vulners.com/cve/CVE-2022-37436
| CVE-2022-30556 5.0 https://vulners.com/cve/CVE-2022-30556

| CVE-2022-29404 5.0 https://vulners.com/cve/CVE-2022-29404
| CVE-2022-28614 5.0 https://vulners.com/cve/CVE-2022-28614
| CVE-2022-26377 5.0 https://vulners.com/cve/CVE-2022-26377
| CVE-2022-22719 5.0 https://vulners.com/cve/CVE-2022-22719
| CVE-2021-34798 5.0 https://vulners.com/cve/CVE-2021-34798
| CVE-2021-26690 5.0 https://vulners.com/cve/CVE-2021-26690
| CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934
| CVE-2019-17567 5.0 https://vulners.com/cve/CVE-2019-17567
| CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220
| CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199
| CVE-2018-1303 5.0 https://vulners.com/cve/CVE-2018-1303
| CVE-2017-9798 5.0 https://vulners.com/cve/CVE-2017-9798
| CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710
| CVE-2016-8743 5.0 https://vulners.com/cve/CVE-2016-8743
| CVE-2016-2161 5.0 https://vulners.com/cve/CVE-2016-2161
| CVE-2016-0736 5.0 https://vulners.com/cve/CVE-2016-0736
| CVE-2015-3183 5.0 https://vulners.com/cve/CVE-2015-3183
| CVE-2015-0228 5.0 https://vulners.com/cve/CVE-2015-0228
| CVE-2014-3583 5.0 https://vulners.com/cve/CVE-2014-3583
| CVE-2014-3581 5.0 https://vulners.com/cve/CVE-2014-3581
| CVE-2014-0231 5.0 https://vulners.com/cve/CVE-2014-0231
| CVE-2013-5704 5.0 https://vulners.com/cve/CVE-2013-5704
| CVE-2006-20001 5.0 https://vulners.com/cve/CVE-2006-20001
| CNVD-2023-93320 5.0 https://vulners.com/cnvd/CNVD-2023-93320
| CNVD-2023-80558 5.0 https://vulners.com/cnvd/CNVD-2023-80558
| CNVD-2022-73122 5.0 https://vulners.com/cnvd/CNVD-2022-73122
| CNVD-2022-53584 5.0 https://vulners.com/cnvd/CNVD-2022-53584
| CNVD-2022-53582 5.0 https://vulners.com/cnvd/CNVD-2022-53582
| CNVD-2022-03223 5.0 https://vulners.com/cnvd/CNVD-2022-03223
| C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B 5.0 https://vulners.com/githubexploit/C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B *EXPLOIT*
| BD3652A9-D066-57BA-9943-4E34970463B9 5.0 https://vulners.com/githubexploit/BD3652A9-D066-57BA-9943-4E34970463B9 *EXPLOIT*
| B0208442-6E17-5772-B12D-B5BE30FA5540 5.0 https://vulners.com/githubexploit/B0208442-6E17-5772-B12D-B5BE30FA5540 *EXPLOIT*
| A820A056-9F91-5059-B0BC-8D92C7A31A52 5.0 https://vulners.com/githubexploit/A820A056-9F91-5059-B0BC-8D92C7A31A52 *EXPLOIT*
| 9814661A-35A4-5DB7-BB25-A1040F365C81 5.0 https://vulners.com/githubexploit/9814661A-35A4-5DB7-BB25-A1040F365C81 *EXPLOIT*
| 5A864BCC-B490-5532-83AB-2E4109BB3C31 5.0 https://vulners.com/githubexploit/5A864BCC-B490-5532-83AB-2E4109BB3C31 *EXPLOIT*
| 17C6AD2A-8469-56C8-BBBE-1764D0DF1680 5.0 https://vulners.com/githubexploit/17C6AD2A-8469-56C8-BBBE-1764D0DF1680 *EXPLOIT*
| 1337DAY-ID-28573 5.0 https://vulners.com/zdt/1337DAY-ID-28573 *EXPLOIT*
| 1337DAY-ID-26574 5.0 https://vulners.com/zdt/1337DAY-ID-26574 *EXPLOIT*
| CVE-2020-11985 4.3 https://vulners.com/cve/CVE-2020-11985
| CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092
| CVE-2018-1302 4.3 https://vulners.com/cve/CVE-2018-1302
| CVE-2018-1301 4.3 https://vulners.com/cve/CVE-2018-1301
| CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975
| CVE-2015-3185 4.3 https://vulners.com/cve/CVE-2015-3185
| CVE-2014-8109 4.3 https://vulners.com/cve/CVE-2014-8109
| CVE-2014-0118 4.3 https://vulners.com/cve/CVE-2014-0118
| 4013EC74-B3C1-5D95-938A-54197A58586D 4.3 https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D *EXPLOIT*
| 1337DAY-ID-33575 4.3 https://vulners.com/zdt/1337DAY-ID-33575 *EXPLOIT*
| CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283
| CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612
|_ PACKETSTORM:140265 0.0 https://vulners.com/packetstorm/PACKETSTORM:140265 *EXPLOIT*
| http-enum:
| /wordpress/: Blog

```
|   /wordpress/wp-login.php: Wordpress login page.
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /manual/: Potentially interesting folder
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=066-066-066-008.res.spectrum.com
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://066-066-066-008.res.spectrum.com:80/
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?
u=1462626880ade1ac87bd9c93a&id=92a4423d01
|
|     Path: http://066-066-066-008.res.spectrum.com:80/index.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?
u=1462626880ade1ac87bd9c93a&id=92a4423d01
|
|     Path: http://066-066-066-008.res.spectrum.com:80/team.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?
u=1462626880ade1ac87bd9c93a&id=92a4423d01
|
|     Path: http://066-066-066-008.res.spectrum.com:80/contact.php
|     Form id: myform
|     Form action:
|
|     Path: http://066-066-066-008.res.spectrum.com:80/contact.php
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?
u=1462626880ade1ac87bd9c93a&id=92a4423d01
|
|     Path: http://066-066-066-008.res.spectrum.com:80/wordpress/
|     Form id: search-form-65a28fc34aafd
|_    Form action: http://raven.local/wordpress/
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4       111/tcp   rpcbind
|   100000  2,3,4       111/udp   rpcbind
|   100000  3,4         111/tcp6  rpcbind
|   100000  3,4         111/udp6  rpcbind
|   100024  1         37633/tcp   status
|   100024  1         47379/udp   status
|   100024  1         51051/tcp6  status
|_  100024  1         60534/udp6  status
MAC Address: 08:00:27:64:D3:43 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 11:27
Completed NSE at 11:27, 0.00s elapsed
Initiating NSE at 11:27
Completed NSE at 11:27, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 40.56 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.040KB)
```

Wordpress

└─$ wpscan --url http://66.66.66.8/wordpress –enumerate vp,vt,u

---

```
__          _______   _____
\ \        / /  __ \ / ____|
 \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
  \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
   \  /\  /  | |     ____) | (__| (_| | | | |
    \/  \/   |_|    |_____/ \___|\__,_|_| |_|
```

WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://66.66.66.8/wordpress/ [66.66.66.8]
[+] Started: Sat Jan 13 16:16:40 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://66.66.66.8/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 | - http://codex.wordpress.org/XML-RPC_Pingback_API
 | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 | - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://66.66.66.8/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://66.66.66.8/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 | - https://www.iplocation.net/defend-wordpress-from-ddos
 | - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.23 identified (Outdated, released on 2023-10-12).
 | Found By: Emoji Settings (Passive Detection)
 | - http://66.66.66.8/wordpress/, Match: '-release.min.js?ver=4.8.23'
 | Confirmed By: Meta Generator (Passive Detection)
 | - http://66.66.66.8/wordpress/, Match: 'WordPress 4.8.23'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00
<==
==
====================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sat Jan 13 16:16:48 2024
[+] Requests Done: 164
[+] Cached Requests: 4
[+] Data Sent: 42.458 KB
[+] Data Received: 185.136 KB
[+] Memory used: 220.844 MB
[+] Elapsed time: 00:00:08

Info Importante

PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp open http   Apache httpd 2.4.10 ((Debian))
111/tcp open rpcbind 2-4 (RPC #100000)
MAC Address: 08:00:27:64:D3:43 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

nikto

```
┌──(kali㉿kali)-[~/Desktop/Raven]
└─$  nikto -h 66.66.66.8 -o nikto_raven.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          66.66.66.8
+ Target Hostname:    66.66.66.8
+ Target Port:        80
+ Start Time:         2024-01-13 11:38:29 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 41b3, size: 5734482bdcb00, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /img/: Directory indexing found.
+ /img/: This might be interesting.
+ /manual/: Web server manual found.
+ /manual/images/: Directory indexing found.
+ /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Configure Apache to ignore this file or upgrade to a newer version. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1446
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /wordpress/wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version usually matches the WordPress version.
+ /wordpress/wp-links-opml.php: This WordPress script reveals the installed version.
+ /wordpress/: Drupal Link header found with value: <http://raven.local/wordpress/index.php/wp-json/>; rel="https://api.w.org/". See: https://www.drupal.org/
+ /wordpress/: A Wordpress installation was found.
+ /wordpress/wp-login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wordpress/wp-login.php: Wordpress login found.
+ 8047 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2024-01-13 12:04:42 (GMT-5) (1573 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```