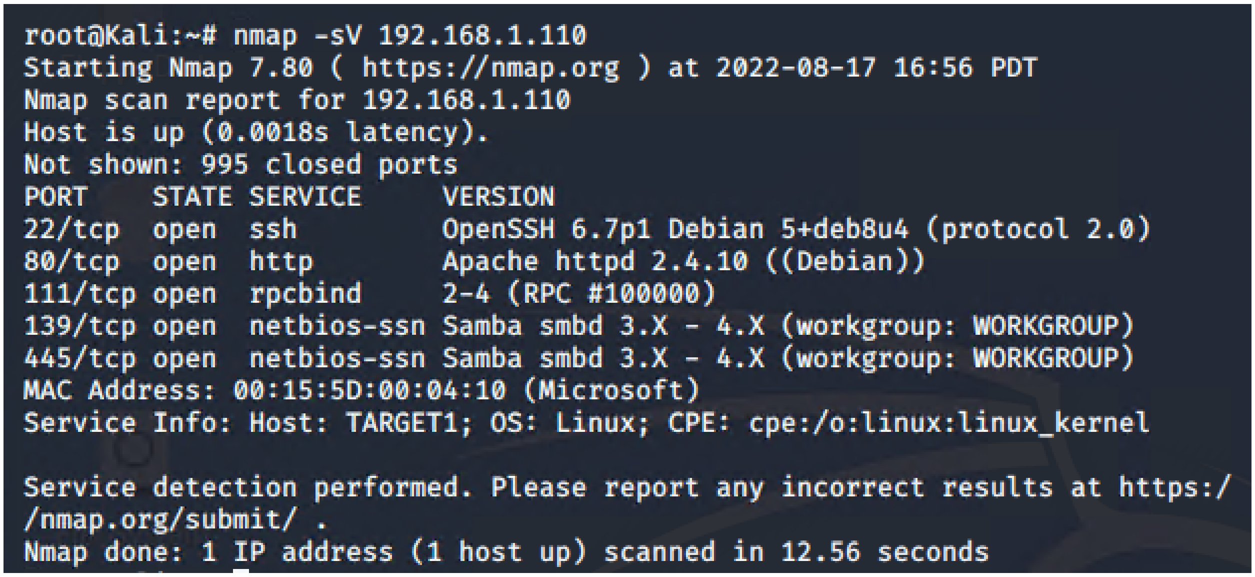
Table of Contents

Exposed Services

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



```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-17 16:56 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0018s 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 12.56 seconds
```

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

- Target 1
    - Port 22/TCP Open SSH
    - Port 80/TCP Open HTTP
    - Port 111/TCP Open rcpbind
    - Port 139/TCP Open netbios-ssn
    - Port 445/TCP Open netbios-ssn

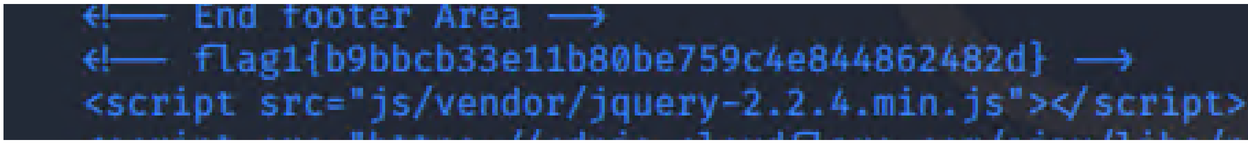
The following vulnerabilities were identified on each target:

- Target 1
    - User Privilege escalation
    - Wordpress database uses unsalted password hash
    - Weak user password
    - User Enumeration

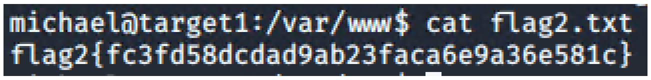
Exploitation

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

- Target 1
  - flag1.txt:

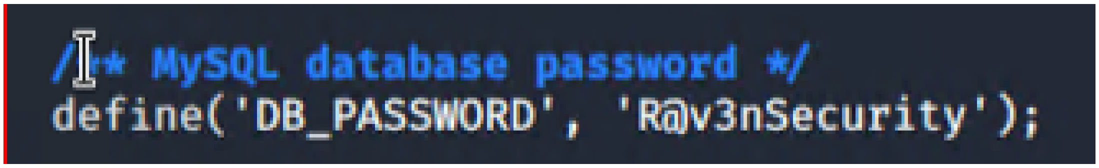
    

    ```
    <!— End footer Area —>
    <!— flag1{b9bbcb33e11b80be759c4e844862482d} —>
    <script src="js/vendor/jquery-2.2.4.min.js"></script>
    ```

    - Exploit Used
    - `ssh michael@192.168.1.110`
      - “michael” password
    - `cd /var/www`
    - `grep *flag`
  - Flag2.txt:
  - 

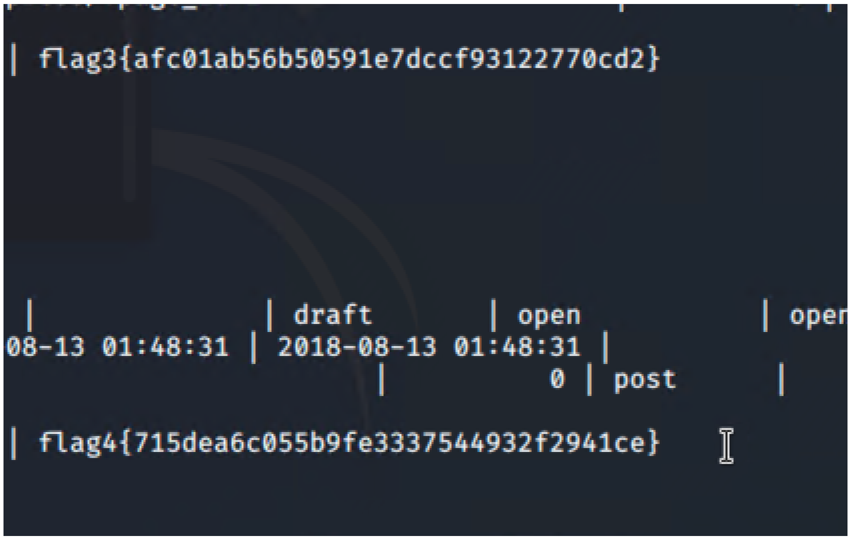
    ```
    michael@target1:/var/www$ cat flag2.txt
    flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
    ```

    - `ssh michael@192.168.1.110`
    - `cd /var/www`
    - `cat flag2.txt`
  - Flag3.txt
    - F
    - Once ssh’d into michael searched the MySQL database to find flag 3 in the /wordpress directory
    - Searching the wp-config.php file will reveal the MySQL credentials:

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

    - These credentials can be used to log into MySQL and access password hashes
    - Once access to MySQL has been granted, selecting from wp_posts; both flag 3 and 4 can be seen

- 

```
| flag3{afc01ab56b50591e7dccf93122770cd2}




 |               | draft        | open            | open
08-13 01:48:31 | 2018-08-13 01:48:31 |
                       |          0 | post       |

| flag4{715dea6c055b9fe3337544932f2941ce}
```