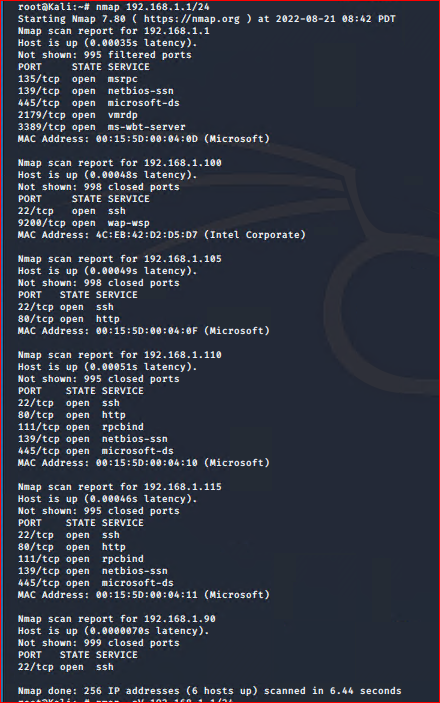
# **Red Team: Summary of Operations**

## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

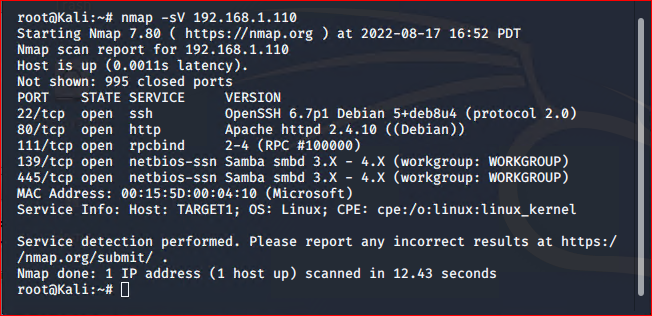


This scan identifies the services below as potential points of entry:

* 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

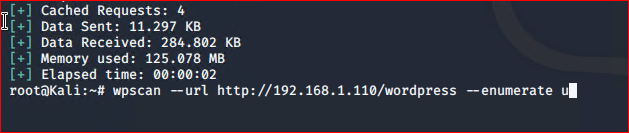
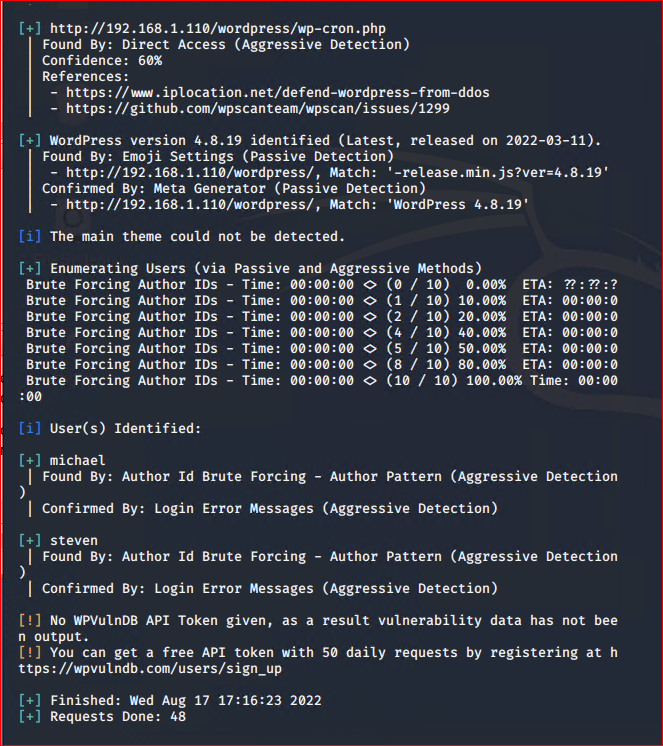
**

### **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*](http://192.168.1.110/wordpress) *–enumerate u*

[**](http://192.168.1.110/wordpress)

**

**

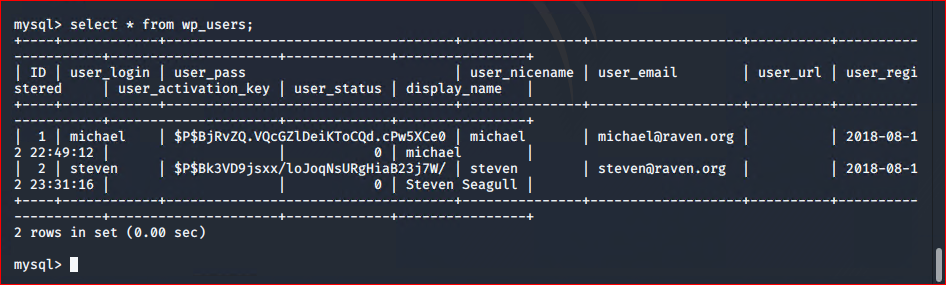
* + flag2.txt: fc3fd*58dcdad9ab23faca6e9a36e581c*
    - **Weak Password**
      * *Michael password was guessed on the second try since it is just his name in all lower case letters*
      * *command: locate \*flag\*.txt was used to find flag 2*

**

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

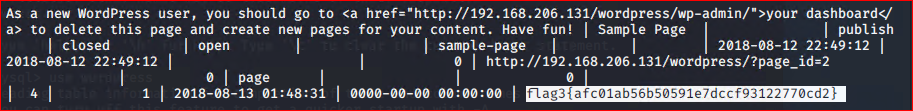
**

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

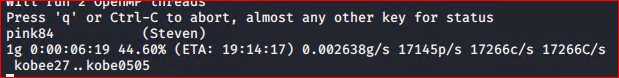
**

* *The third flag was also found within the table wp\_posts*
  + *select \*from wp\_posts*

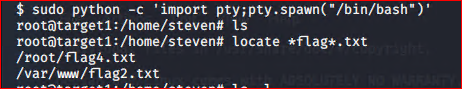
**

**

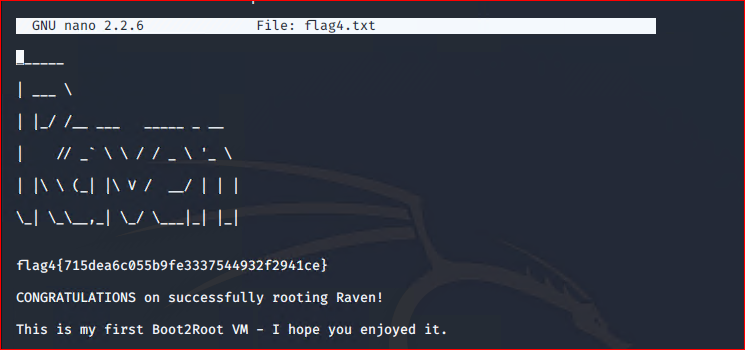
* + flag4.txt: 715dea6c055b9fe3337544932f2941ce
    - **Privilege Escalation**
      * Cracked Steven’s password with:
        + john –wordlist=’/usr/share/wordlists/rockyou.txt” usr hashes.txt



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

**

* + - * *sudo python -c ‘import pty;pty.spwan(“bin/bash”)’*

**