# **Red Team: Summary of Operations**

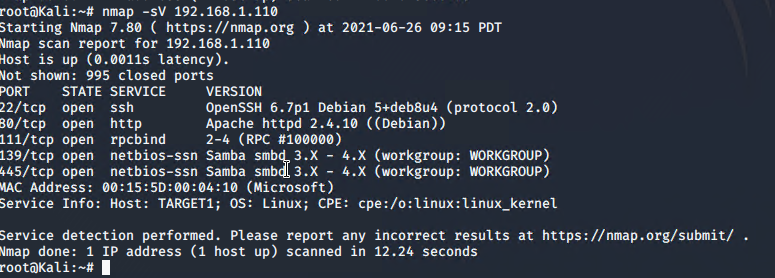
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

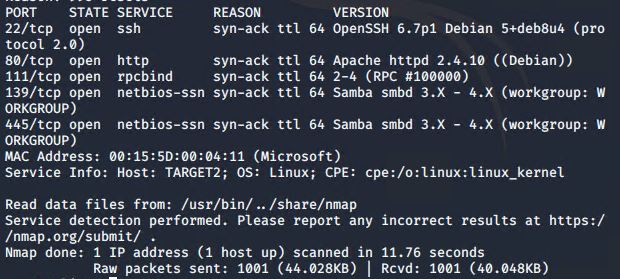
### **Exposed Services**

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

**Target 1:** $ nmap -sV 192.168.1.110



**Target 2:** $ nmap -sV -vvv --version-intensity 9 192.168.1.115



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

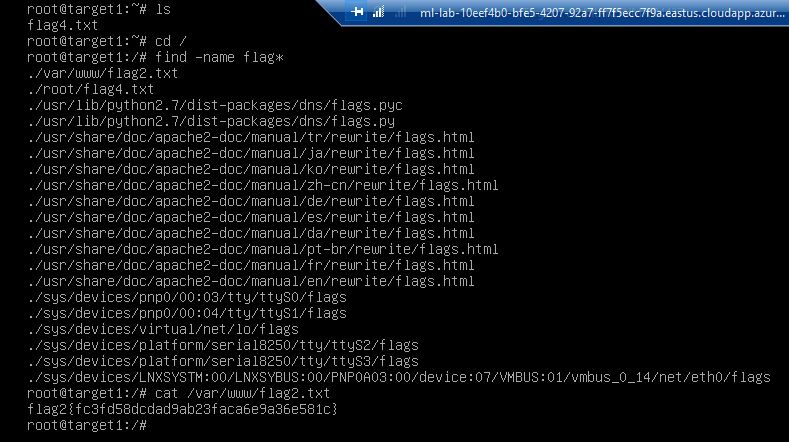
* Target 1 and Target 2
  + SMB
  + WordPress Server
  + SSH open to external IPs

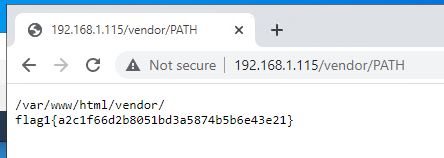
The following vulnerabilities were identified on each target:

* Target 1
  + Default credentials - root/toor
  + WordPress - Improper Error Handling - User Enumeration
  + Optionsbleed Bug - CVE 2017-9798
  + Arbitrary Module Load - CVE 2017-7494
* Target 2
  + Weak/Reused Credentials - vagrant:tnargav stolen from Target 1
  + Optionsbleed Bug - CVE 2017-97998
  + Arbitrary Module Load - CVE 2017-7494

### **Exploitation**

The Red Team was able to penetrate Target 1 and Target 2 and retrieve the following confidential data:

* Target 1
  + flag1.txt: b9bbcb33e11b80be759c4e844862482d
  + 
    - **Inspected Source on WordPress site**
      * Ctl+f and search for ‘flag’
  + flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c
  + 
    - **Default Credentials**
      * Logged into target 1 using root:toor
      * find -name flag\*
      * 
      * cat /var/www/flag2.txt
  + flag3.txt afc01ab56b50591e7dccf93122770cd2
  + 
    - **No exploit used**
      * Logged into mysql as root
      * Searched through each table until we found flag 3
  + flag4.txt 715dea6c055b9fe3337544932f2941ce
  + 
    - **Default Credentials**
      * Logged into target 1 using root:toor
      * ls to display files and directories
      * cat flag4.txt to display flag
* Target 2
  + Flag 1



Found in 192.168.1.115/vendor/PATH after enumerating with Gobuster.

* + Flag 2



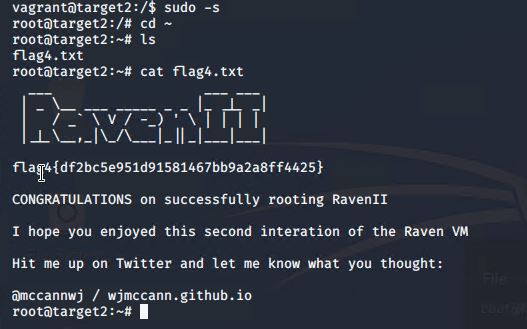
Found the flag in /var/www after using a credential reuse attack, followed by a find command.

* + Flag 3



Found after escalating privileges on Target 2 and using a more complex find command.

* + Flag 4



Found in root’s home directory. We had a feeling about its location based on breaking into Target 1.