# **Red Team: Summary of Operations**

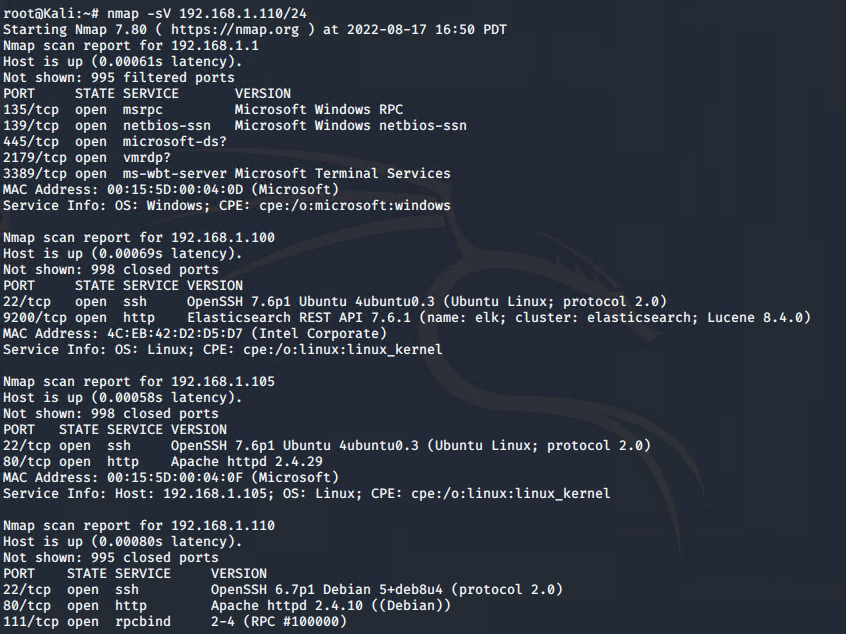
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

Command: nmap -sV 192.168.1.110/24



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

* Target 1 (192.168.1.110)
  + Port 22/tcp OpenSSH

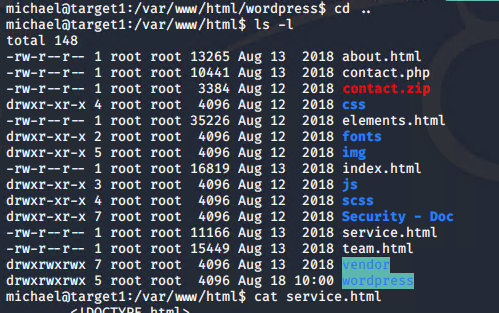
The following vulnerabilities were identified on each target:

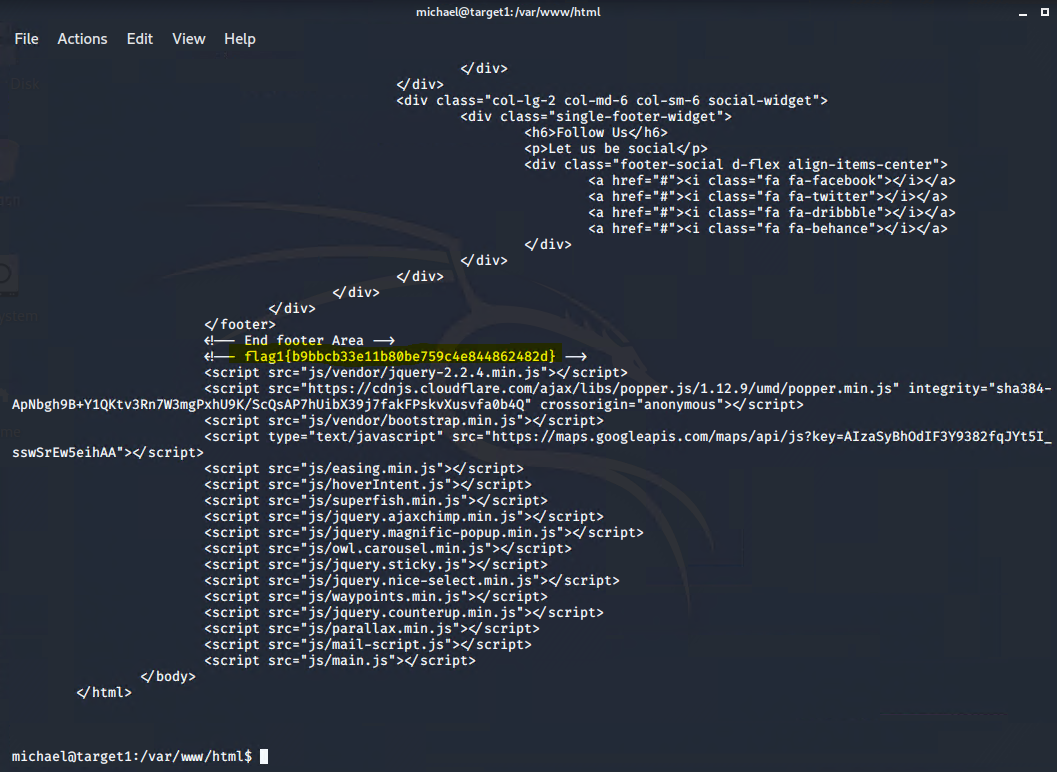
* Target 1
  + Unsecured ports
  + Sensitive Data Exposure
  + Weak Password/Brute Force
  + Unsecured root privileges

### **Exploitation**

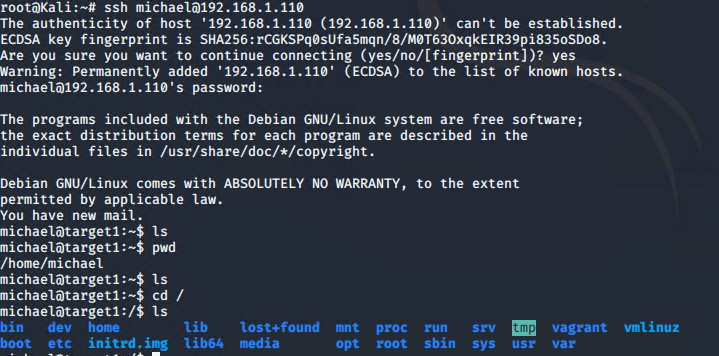
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

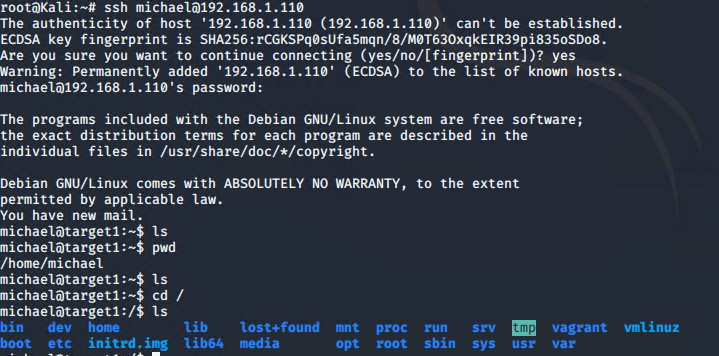
* Target 1
  + flag1.txt:

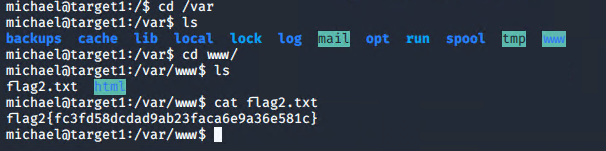




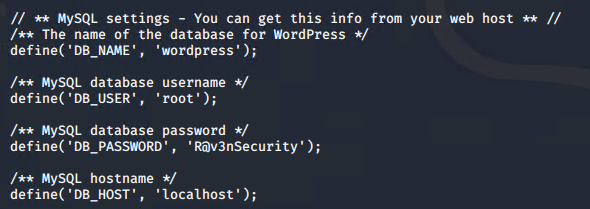
* + - **Exploit Used**
      * After enumerating the WordPress site, Michael’s password was easy to simply guess (password: michael). SSH’d into Targer1 as Michael and navigated to /var/www/html/wordpress
      * Command: wpscan --url 192.168.1.110/wordpress --enurmate u
  + flag2.txt:



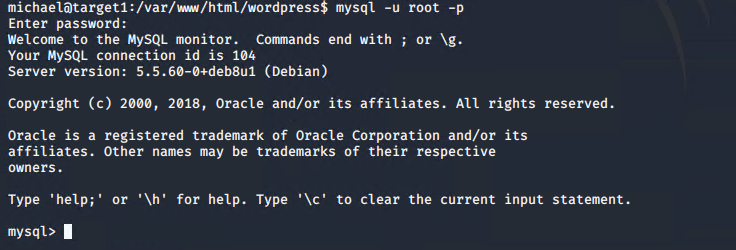


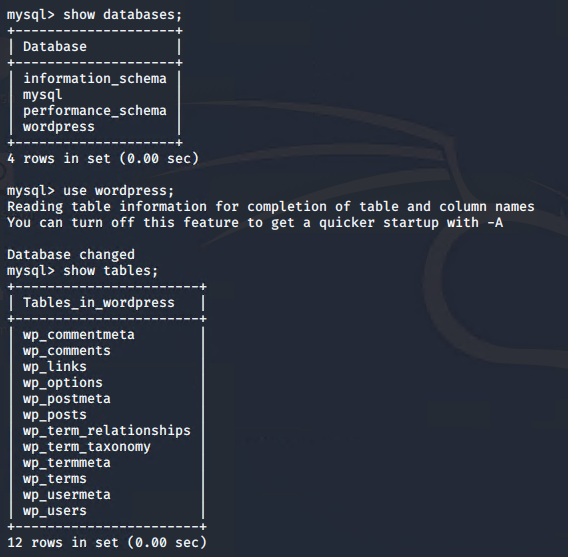


* + - **Exploit Used**
      * After SSH’ing into Target1 as Michael, navigated to /var/www/
* flag3.txt and flag4.txt:
  + The usernames and passwords for the MySQL database was found in the wordpress\_config file

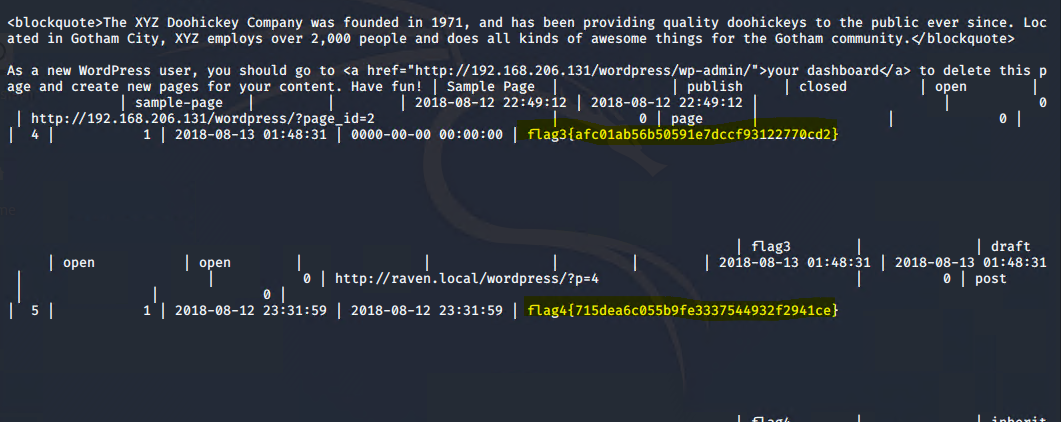


* + Using this information, we logged into the database and found flags 3 and 4 in “wp\_posts”, and hashes for Michael and Steven in “wp\_users”











* flag4.txt:
  + We put the hashes into a “wp\_hashes.txt” file, and used the following John The Ripper to crack Steven’s password (pink84)
    - Command: john wp\_hashes.txt





* + We ssh’d into Target1 using Steven’s password, and used the following command to escalate to root privileges to find flag4.txt
  + sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’

