# **Red Team: Summary of Operations**

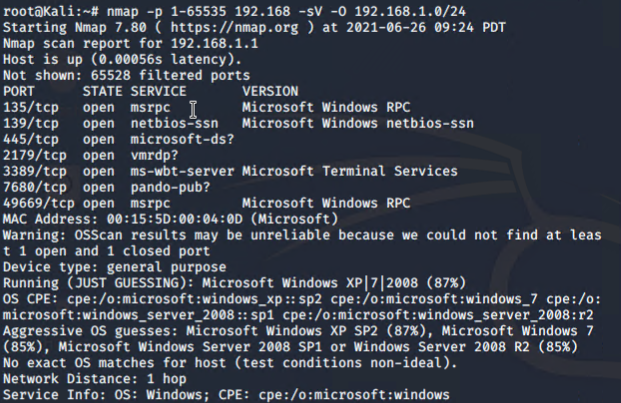
## **Table of Contents**

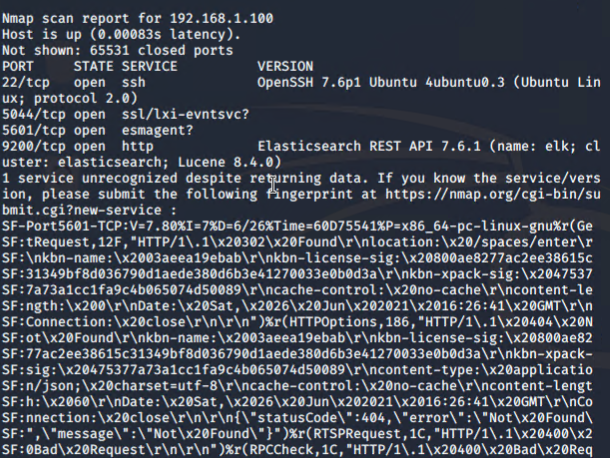
* Exposed Services
* Critical Vulnerabilities
* Exploitation

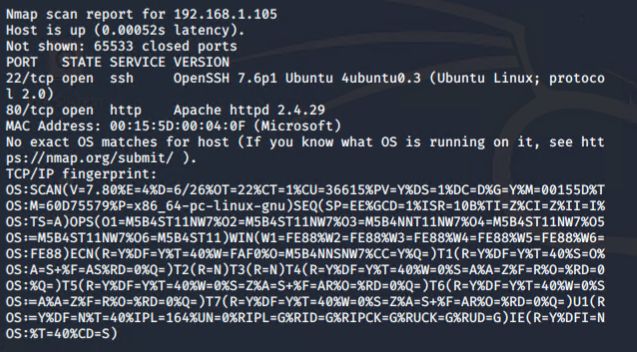
### **Exposed Services**

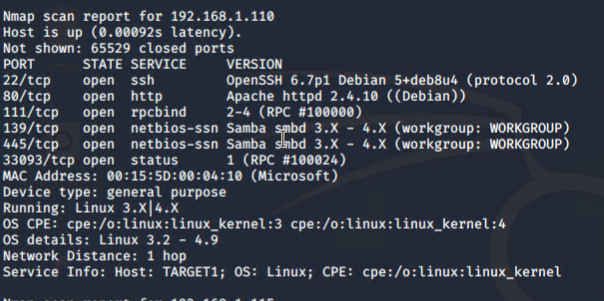
Nmap scan results for each machine reveal the below services and OS details:

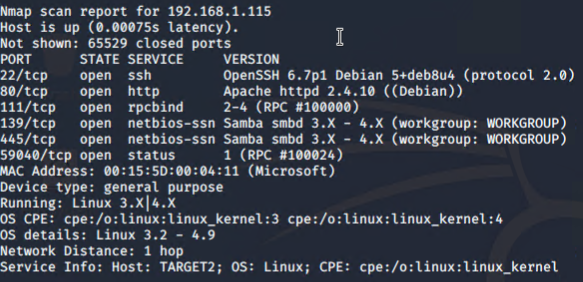
**$ nmap -p 1-65535 -sV -O 192.168.1.0/24**

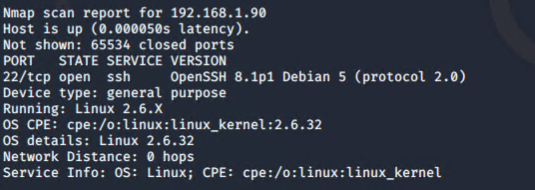




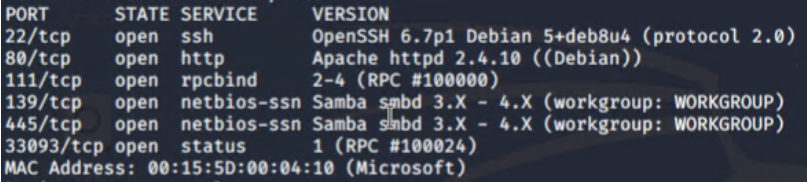








This scan identifies the services below as potential points of entry:

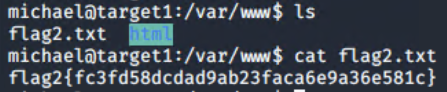
* Target 1 (192.168.1.110)
  + List of exposed services
    - 

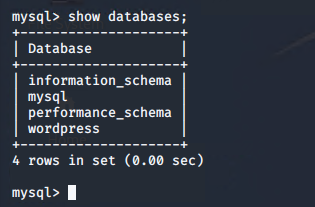
The following vulnerabilities were identified on each target:

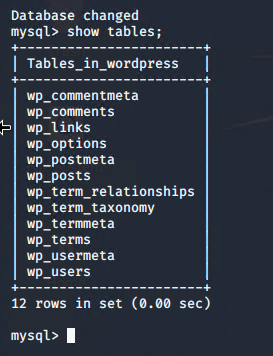
* Target 1
  + **Port Vulns**
    - 111/tcp rpcbind- CVE 2017-8779
    - Medium 4 ~ 6.9 (level of difficulty)
    - An attacker could use this vulnerability to trigger large unfreed memory allocations on the system leading to a remote Denial of Service.
* Target 1
  + **Port Vulns**
    - Port 22/ssh- CVE-2018-6082
    - High - 7.5 (level of difficulty)
    - Allows a remote attacker to potentially enumerate internal host services
* Target 1
  + **Port Vulns**
    - Port 139/445 CVE 2007-3923
    - High 7.8
    - Allows remote attackers to cause a Denial of Service via a flood of TCP SYN packets to port 139 or 445.
* Target 1
  + **User Enumeration**
* Target 1
  + **Unsalted Hash**
* Target 1
  + **Weak PW for user: Michael**
* Target 1
  + **Root privileges on account with weak PW**

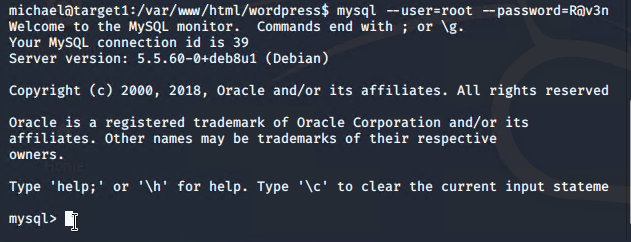
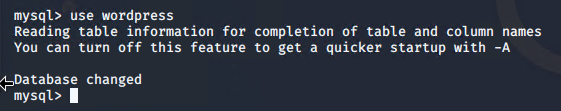
### **Exploitation**

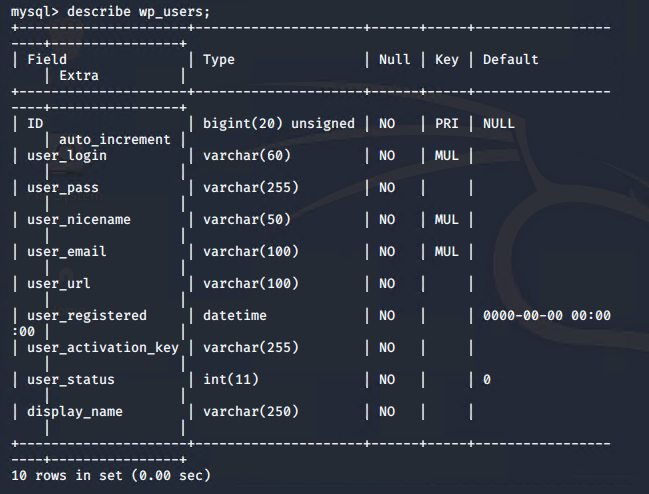
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

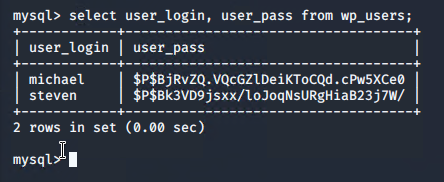
* Target 1
* Flag 1
  + 
    - **Exploit Used**
      * Privileged information in publicly available web spaces
      * Navigated to ‘Services’ page on Raven Security site (192.168.1.110) and right-clicked to view ‘View Page Source’ and then used ‘ctrl + F’ to search for “flag”
* Flag 2
  + - **Exploit Used**
      * Weak and easily guessable password was used to SSH into User: Michael’s account. Once inside Michael’s account, the team was able to search through the user’s files and discover the file “flag2.txt”
      * ssh michael@192.168.1.110
      * Use Linux ‘cd’ command to navigate through directories and ‘cat’ command to return the hash for flag2.txt
* Flag 3
  + 
    - **Exploit Used**
      * Used Michael’s account to navigate to the wp-config.php file containing login information for the MySQL database. After logging into MySQLthe team explored the WordPress data tables, and discovered the wp\_posts table where flag 3 was hidden
      * mysql -u root -p R@v3nSecurity
      * show databases;
      * use wordpress
      * show tables;
      * select \* from wp\_posts;
      * **\*see following nine screenshots\***

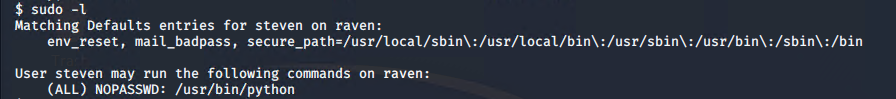
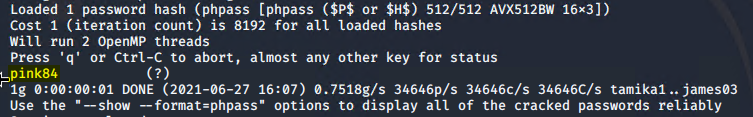






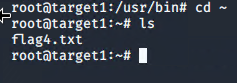








Flag 4

* + 
    - **Exploit Used**
      * Based on the discovery from MySQL wp\_users table, the team was able to discover and crack Steven’s hashed password with John the Ripper and SSH into his account. After logging into Steven’s account, the team discovered that Steven’s account could run Python scripts with privileged escalation.

