# Red Team: Summary of Operations

## 

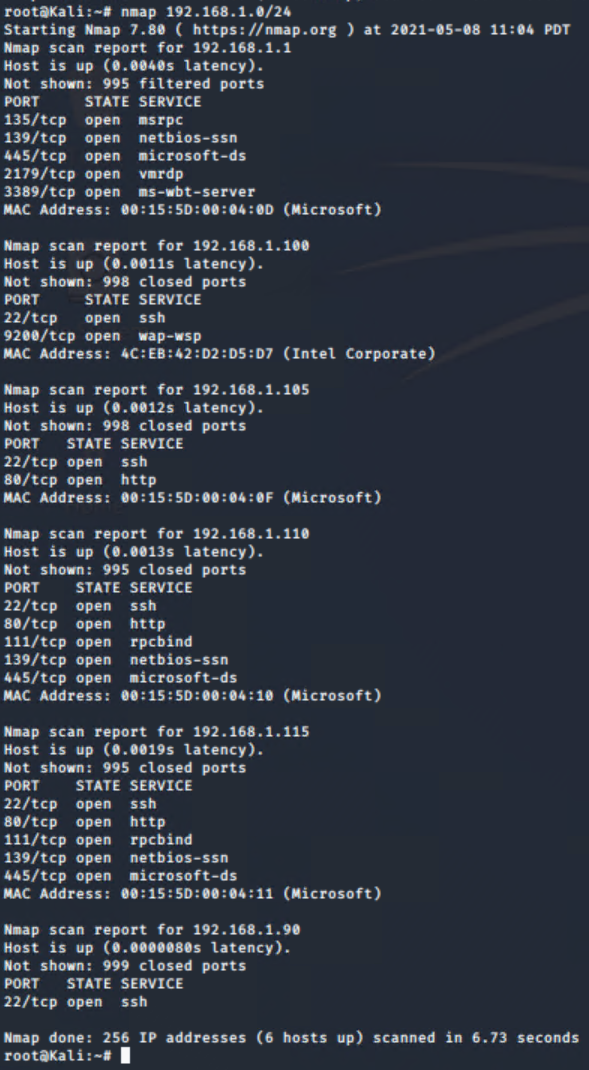
## Table of Contents

* Exposed Services
* Critical Vulnerabilities
* Exploitation

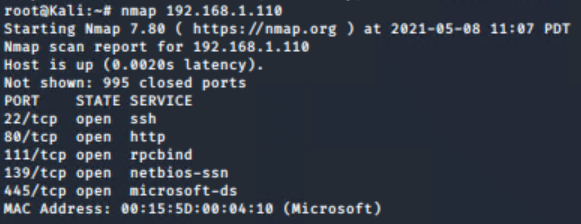
### Exposed Services

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

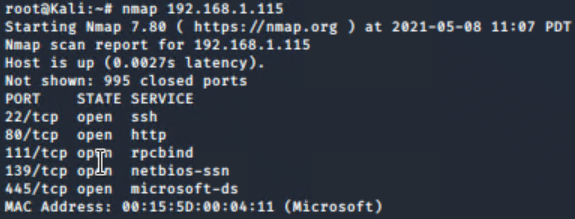
$ nmap 192.168.1.0/24



$ nmap 192.168.1.110



$ nmap 192.168.1.115



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

**Target 1**

1. rpcbind
2. netbios-ssn
3. microsoft-ds

### Critical Vulnerabilities

The following vulnerabilities were identified on each target:

**Target 1**

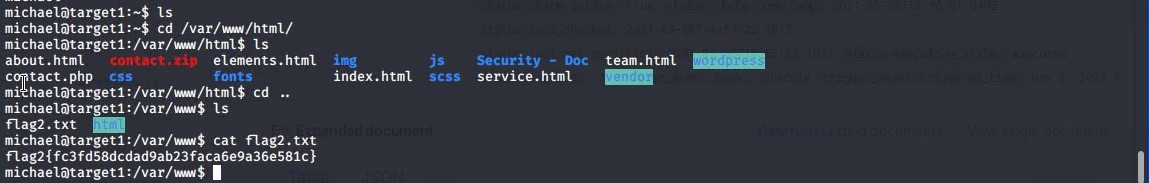
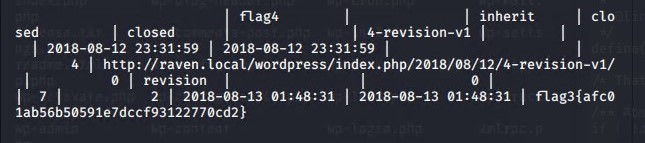
1. OpenSSH 6.7
2. Apache v2.4.10
3. NetBIOS

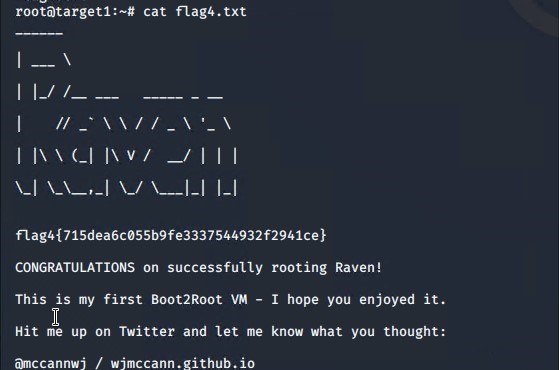
Please see [NMAP Scan](https://docs.google.com/document/d/1xxL5CwTZypfKBTg_akullO1QSMpDiPf6Gj9fFxNxKYc/edit?usp=sharing) for a complete nmap scan.

Exploitation

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

**Target 1**

* Flag 1 
* Exploit Used:
  + Identify the exploit used- The exploit used was taking advantage of a users weak password
  + The commands ran to get into the account to find information and the flags was the use of a wordpress site dump, then guessing the users password (michael) to get into via SSH, then searching in some of the documents to look for information stumbled across flag1, using [cat service.html].
* Flag 2
* Exploit Used:
  + Identify the exploit used- The exploit we used was the same as for flag one and taking advantage of a users weak password.
  + Just as with flag one but jumping down a directory we found the flag2.txt and used the [cat flag2.txt] command to view the contents of the .txt file.
* Flag 3
* Exploit(s) used:
  + After a few more steps we got into the mysql database service moved into the wordpress database and opened several of the tables looking for information. After opening the wp\_posts table flag three and the context were found.
  + The commands run to get here were to open mysql [mysql -u root -p R@v3nSecurity], then changing the database [mysql> use wordpress] then searched the wp\_posts table with [mysql> select \* from wp\_posts;]
* Flag 4



* Exploit(s) used:
  + john to break password hash to gain stevens password, ssh into stevens user profile, escalated privileges via python exploit, and searched for the flag 4.txt file.
  + Commands used getting into stevens user account from root@kali. [ssh steven@192.168.1.110] then we had to escalate user privileges to root using [sudo -c ‘import pty;pty.spawn(“/bin/bash”);’] after that i used the find command for the flag [find ./ -type f -name flag\*] , spit out the information to get to flag4 then we [cat flag4.txt].