# **Red Team: Summary of Operations**

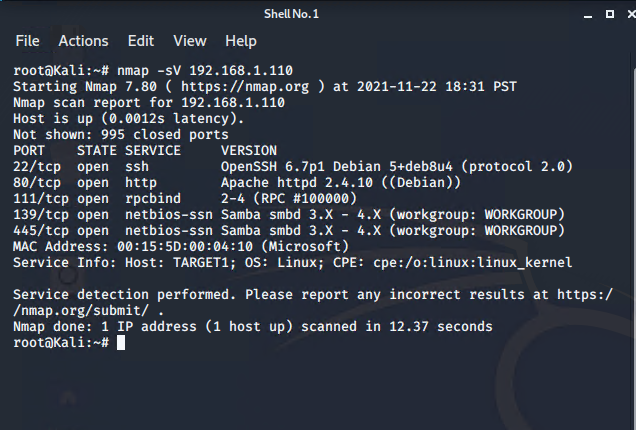
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

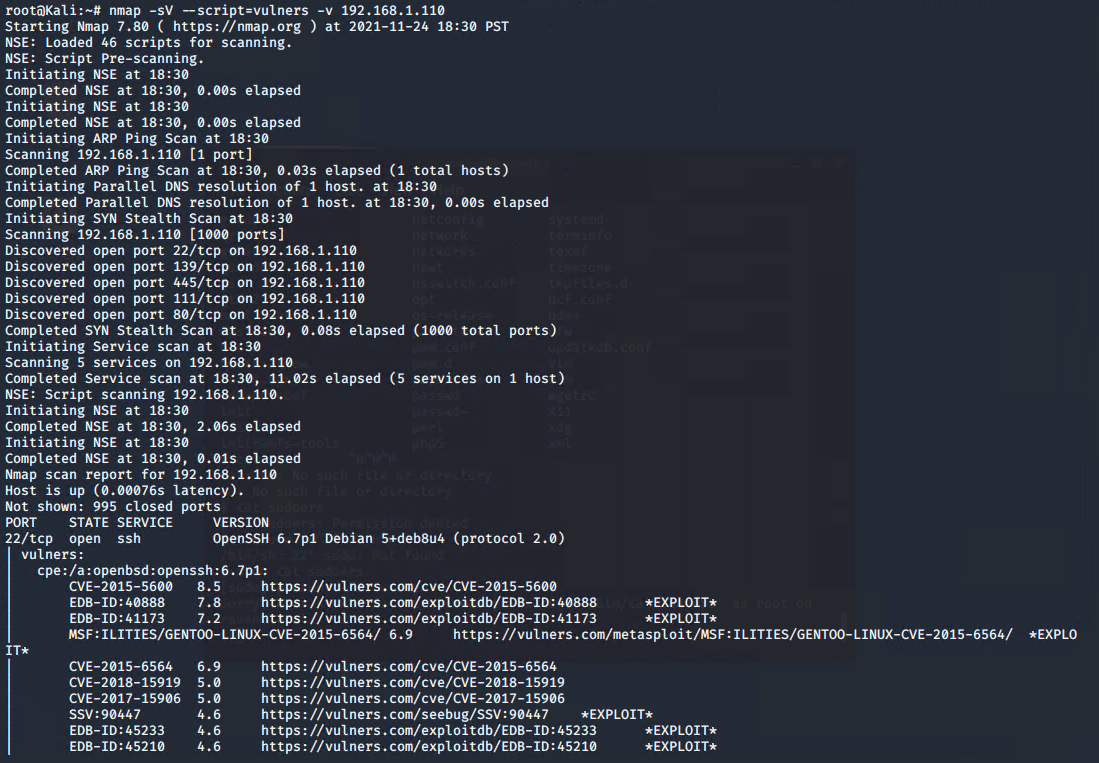
### **Exposed Services**

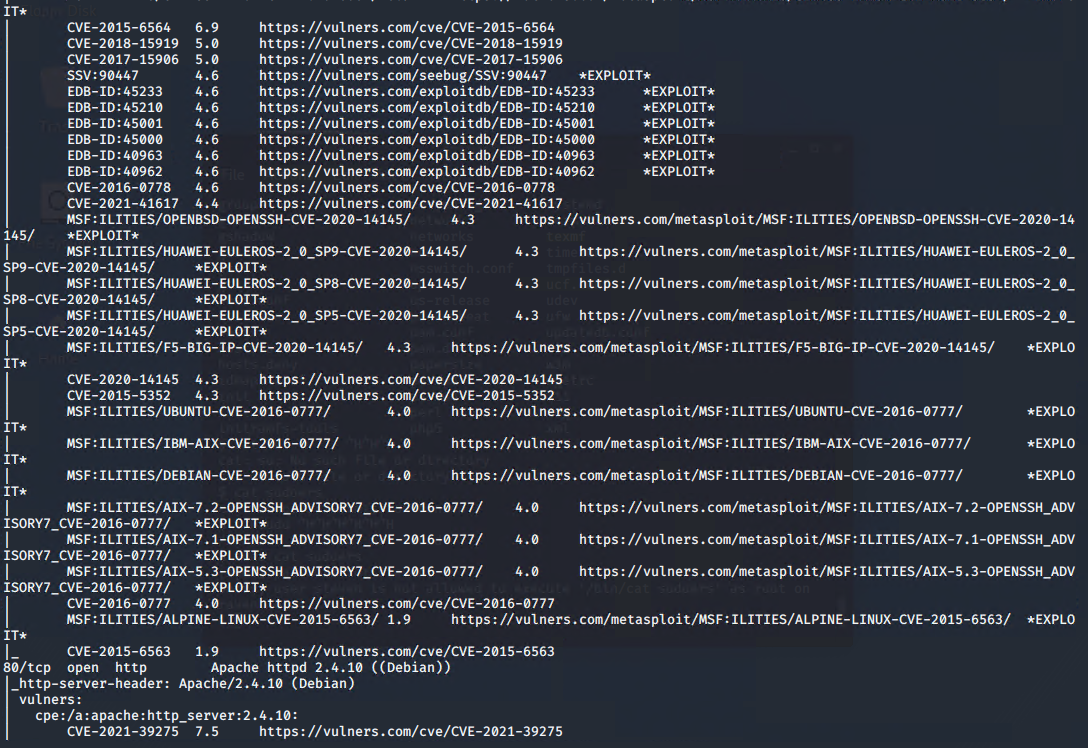
Nmap scan results for each machine reveal the below services and OS details:

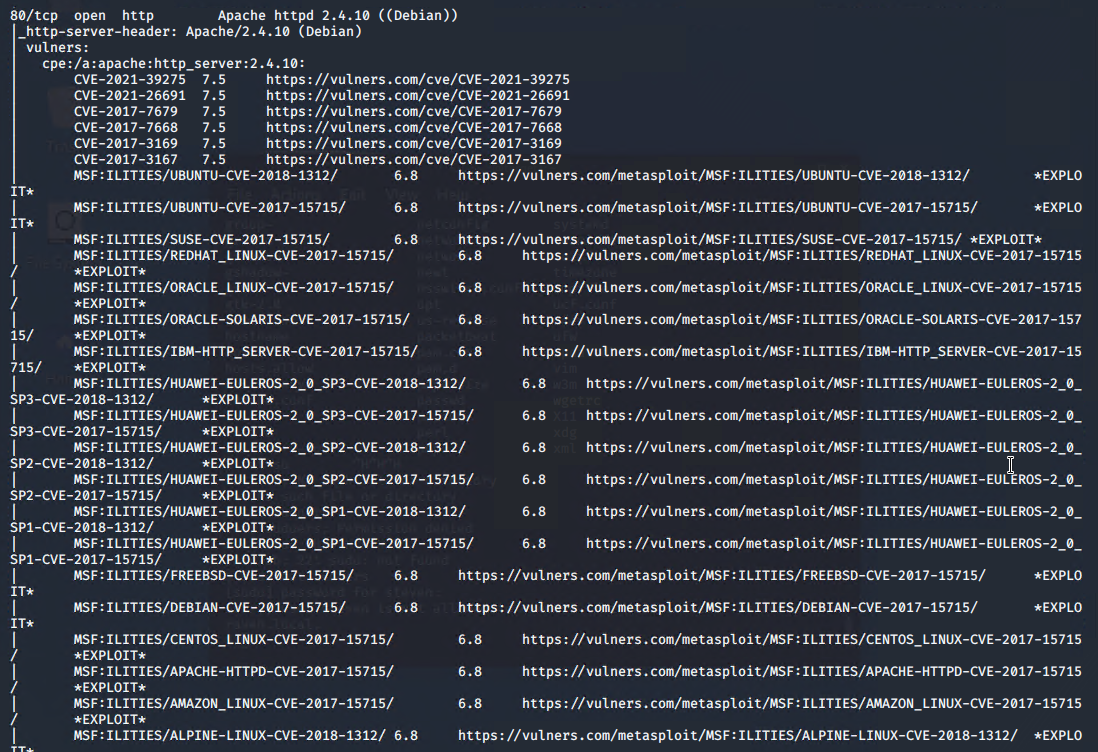
$ nmap -sV 192.168.1.110

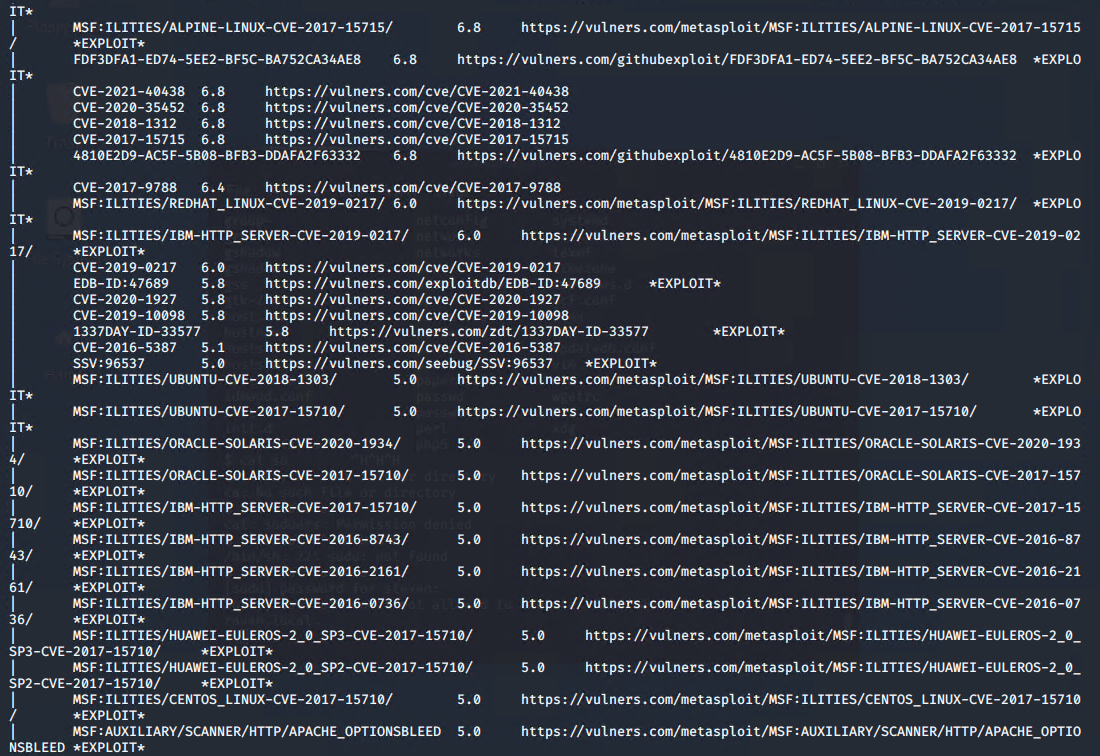


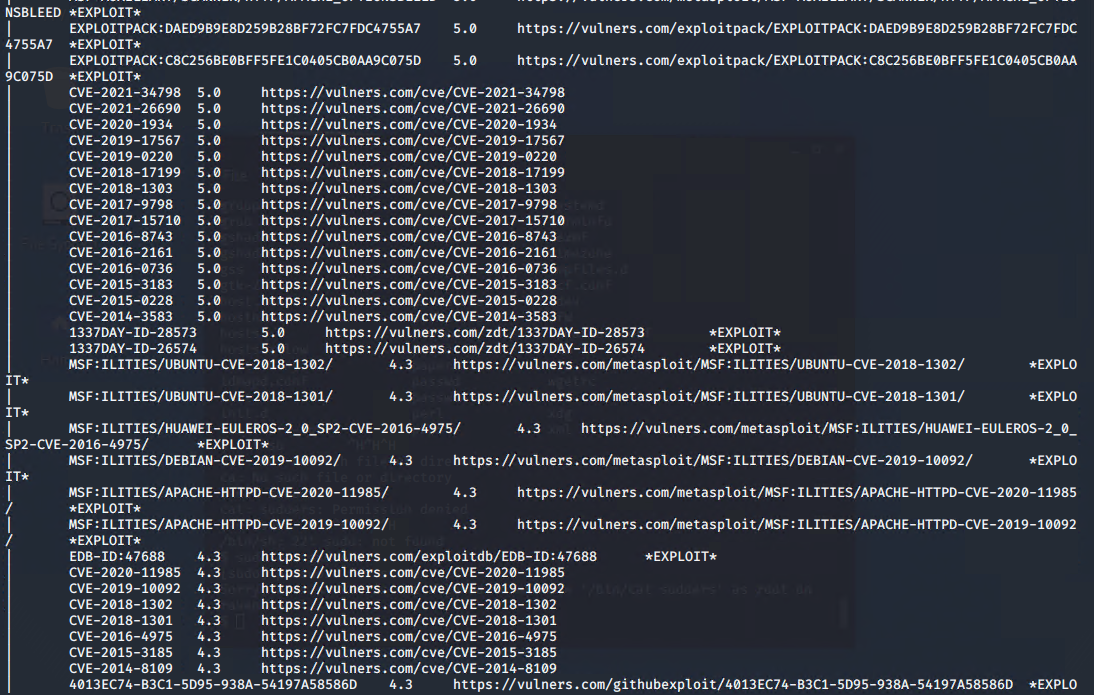
The following vulnerabilities were identified on each target:

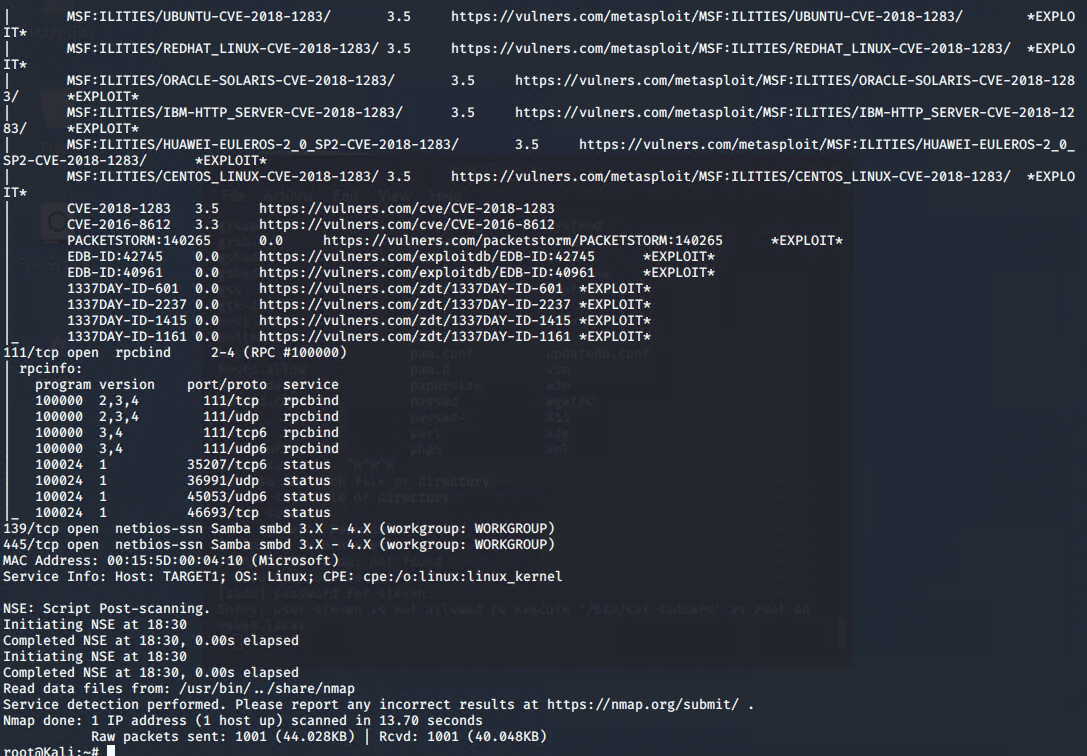












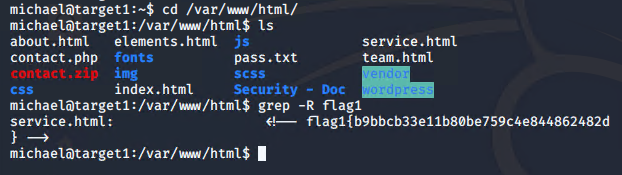
### **Exploitation**

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

* Target 1
  + flag1.txt: *b9bbcb33e11b80be759c4e844862482d*
    - Exploit Used
      * *Use “wpscan --url* [*http://192.168.1.110:80/wordpress*](http://192.168.1.110:80/wordpress) *-e u”*

*To discover users Steven and Michael*

* + - * *Used “ssh michael@192.168.1.110” and guessed password “michael” to gain access to michaels account*
      * *Navigated to /var/www/html and used “grep -R flag1” to find flag 1*

**

* + Flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c
    - Exploit Used
      * *Flag 2 could be found by using “cd ..” to go up one directory, then using “ls” to reveal the file.*
      * *Simply cat the file with “cat flag2.txt” to reveal the hash.*

