# **Red Team: Summary of Operations**

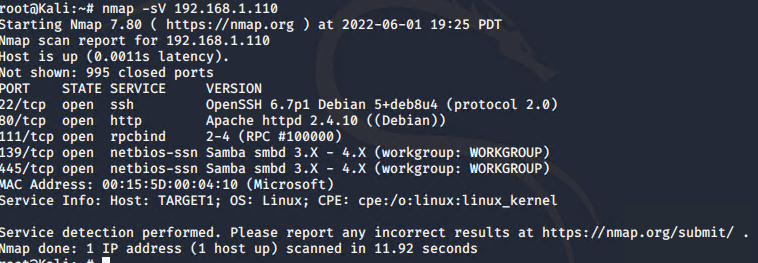
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

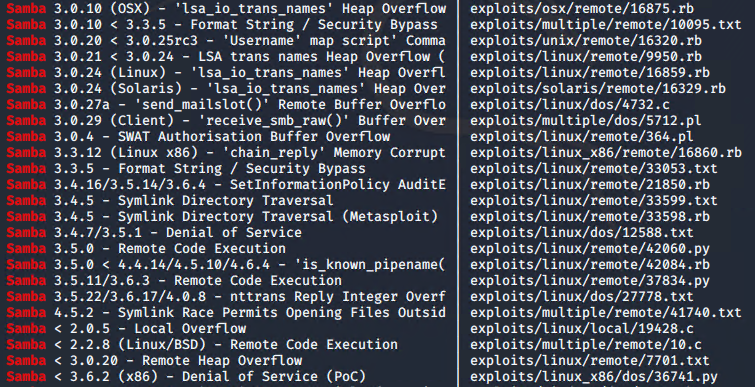
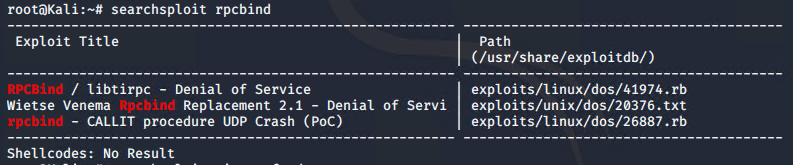
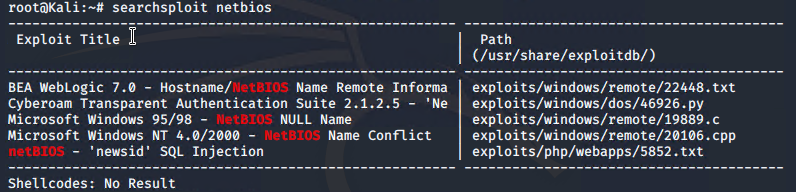
$ nmap -sS -O 192.168.1.110

# 

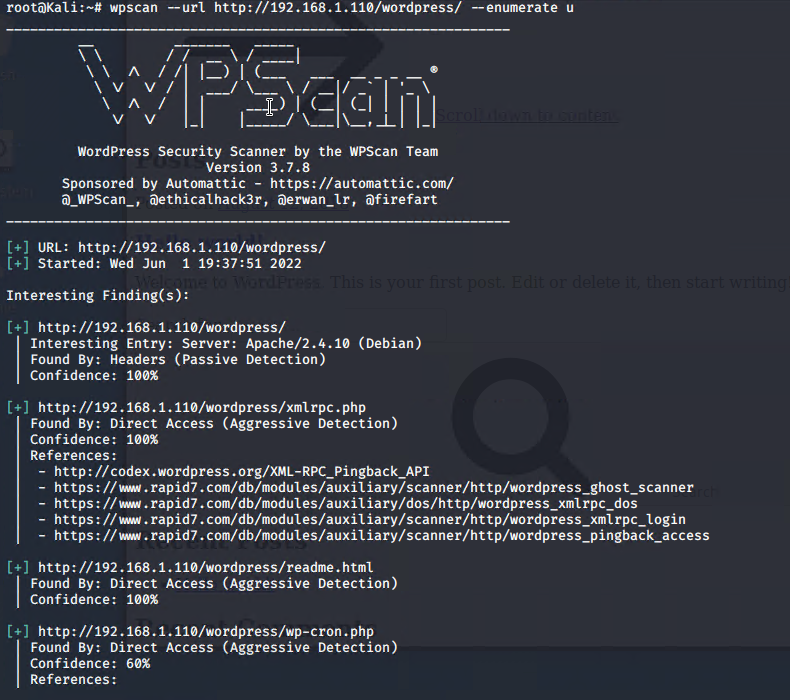
This scan identifies the services below as potential points of entry:

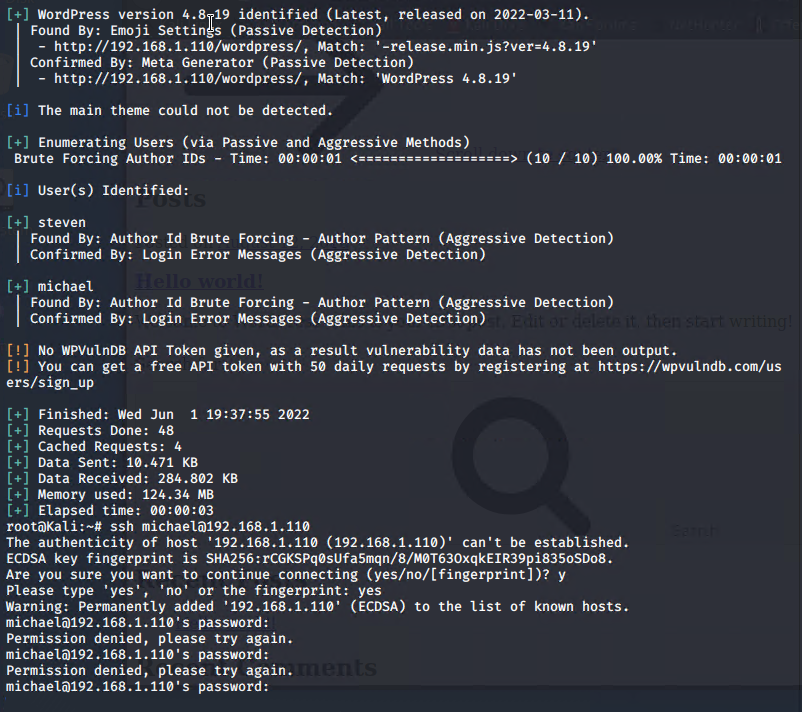
* Target 1
  + SSH port 22
  + Rpcbind port 111
  + Netbios-ssn port 139
  + Microsoft-ds port 445

The following vulnerabilities were identified on each target:

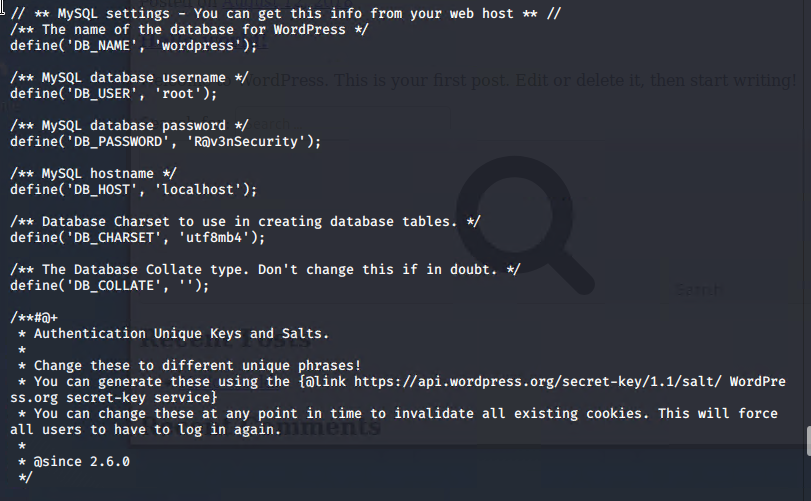
* Target 1
  + Port 22 left exposed
  + Samba Has lots of available exploits
  + 
  + Rpcbind has multiple exploits available
  + 
  + Netbios-ssn has multiple exploits available
  + 

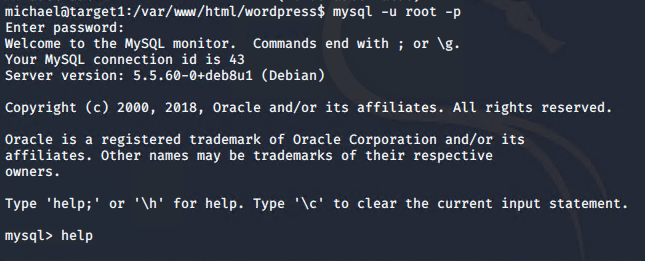
### **Exploitation**

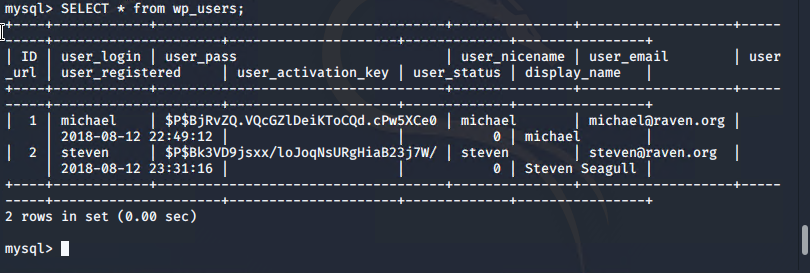
**

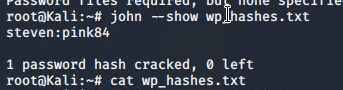
**

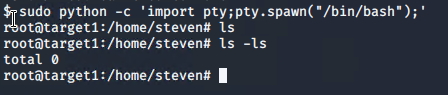
*Michaels password was michael through a guess*

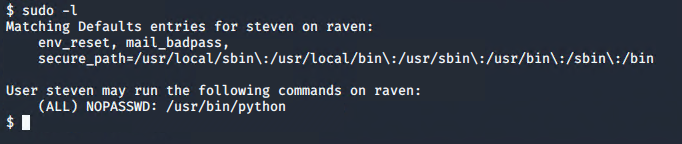
**

**

**

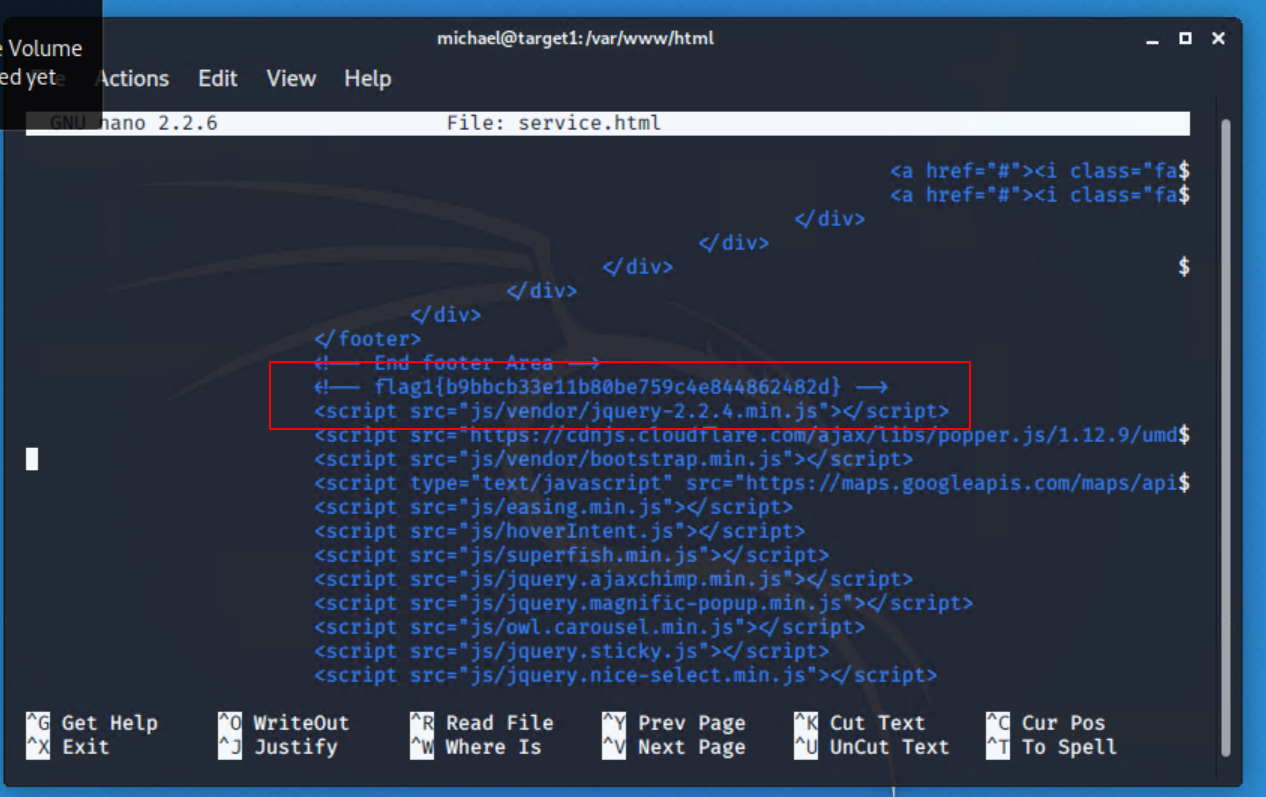
**

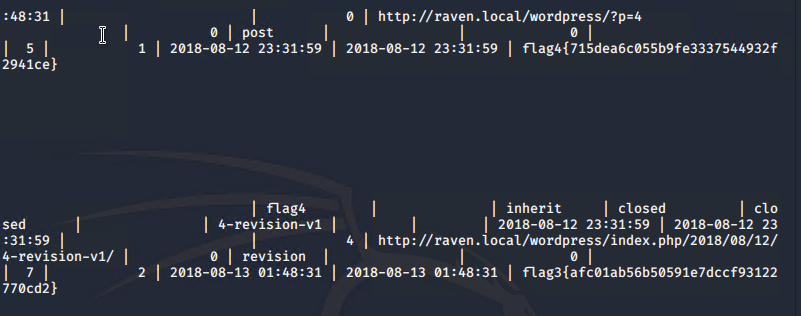
**

**

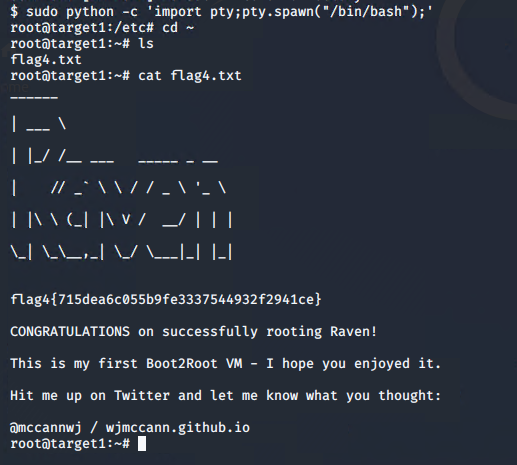
*We can see steven is allowed to use python commands*

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

* Target 1
  + flag1.txt: *b9bbcb33e11b80be859c4e844862482d*
  + **
    - **Exploit Used**
      * *To find the first flag we used wp scan to enumerate the site*
      * *wpscan –url* [*http://192.168.1.110/wordpress/*](http://192.168.1.110/wordpress/) *-enumerate u*
  + flag2.txt: *fc3fd58dcdad9ab24faca6e9a36e581c*
  + **
    - **Exploit Used**
      * *Ssh into michael using ssh*
      * *ssh michael@192.168.1.110 then look around*



From table wp\_posts



Alternately from sudo on steven