# **Red Team: Summary of Operations**

## **Table of Contents**

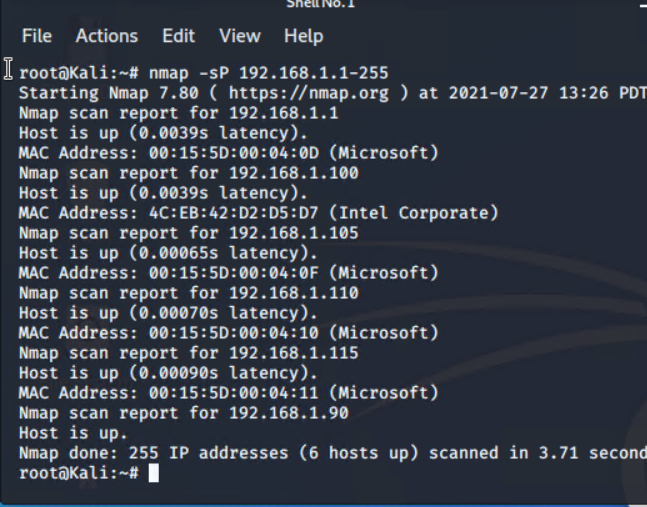
* Exposed Services
* Critical Vulnerabilities
* Exploitation

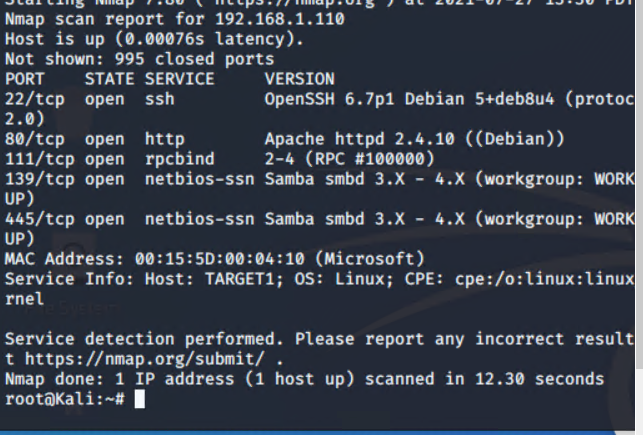
### **Exposed Services**

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

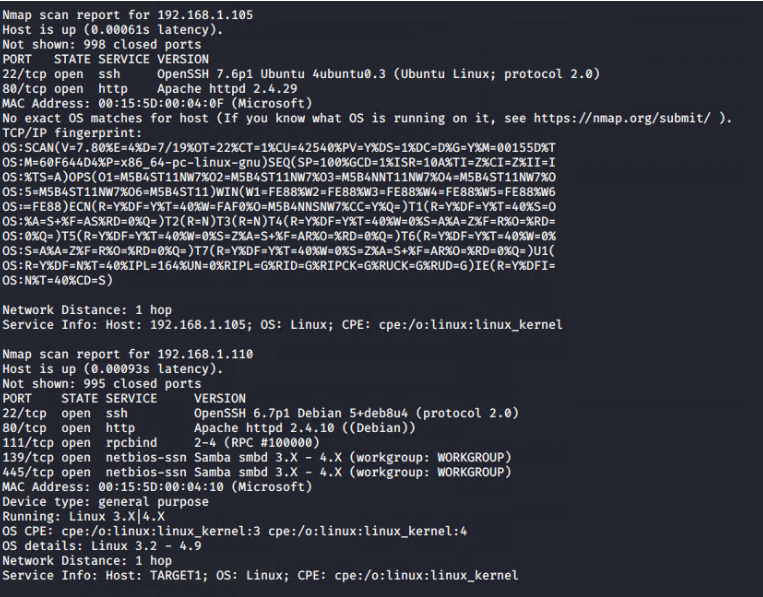
$ nmap -sP 192.168.1.1-255

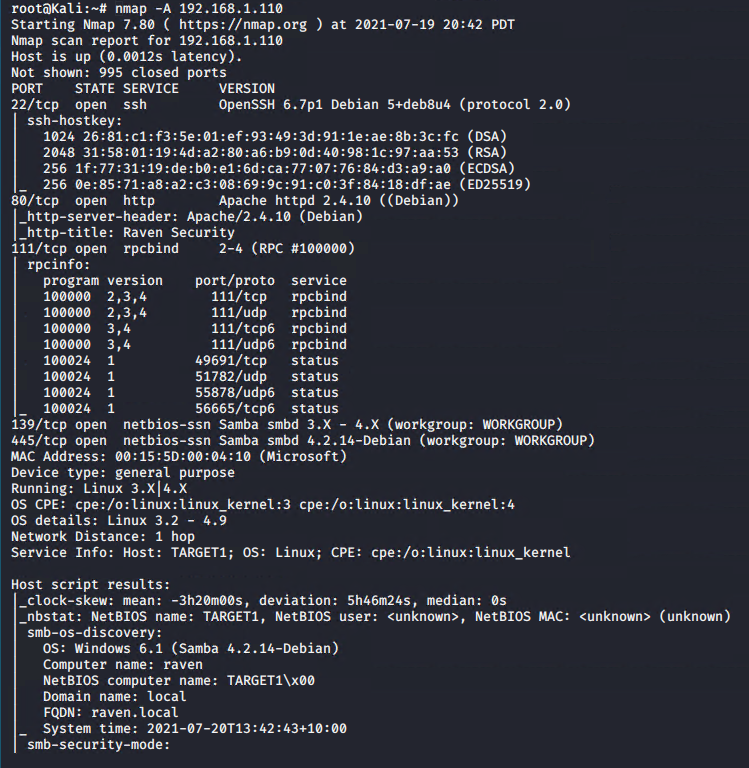
Reveals 192.168.1.110 and 192.168.1.115 are target 1 and target 2.

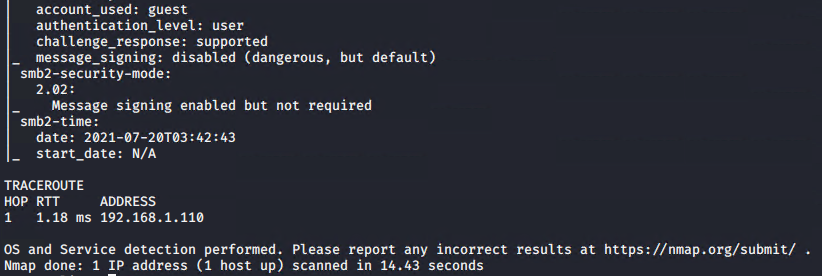




nmap -sV -O 192.168.1.105







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

* Target 1
  + Port 22 (SSH)
  + Port 80 (HTTP)
  + Port 111 (rpcbind)
  + Port 139 (netbios-ssn) version Samba smbd
  + Port 445 (netbios-ssn) version Samba smbd

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

The following vulnerabilities were identified on each target:

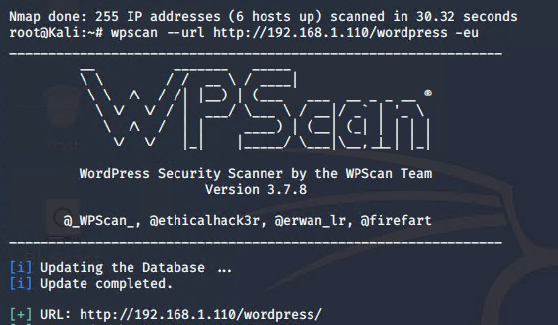
* Target 1
  + Port 22 is open - this provides the ability to ssh in with discovered credentials.
  + Port 80 is open - this provides access to http server

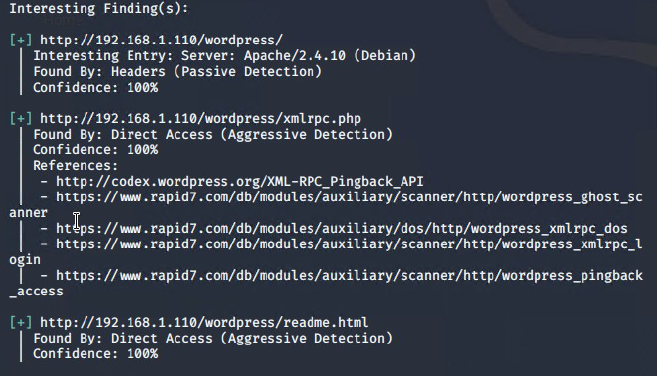
### **Exploitation**

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

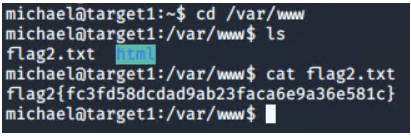
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

* Target 1
  + Wpscan --url <http://192.168.1.110/wordpress> -eu
    - **Exploit Used**

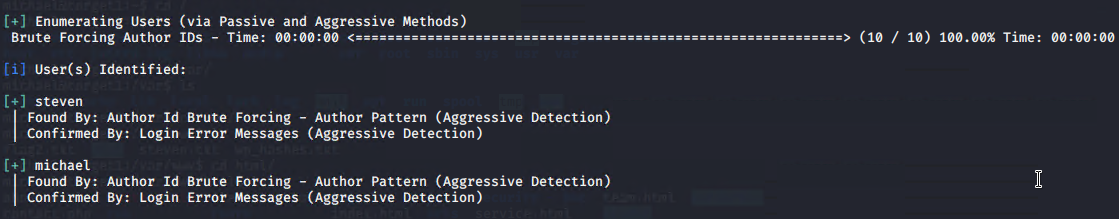




* + - **Exploit Used**

****

****

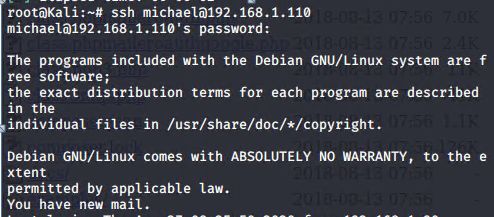


Both Steven and Michael are displayed.

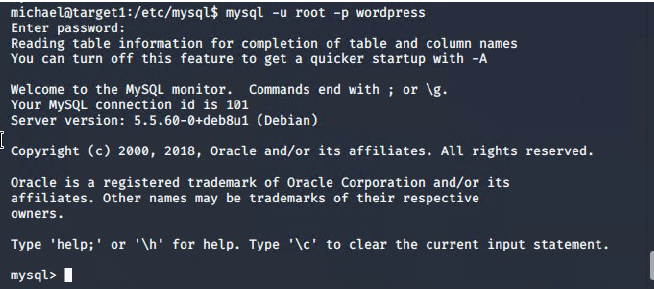
ssh michael@192.168.1.110

Using brute force, the hint was the “easiest” password which was the same as the user name.

Password: “michael”

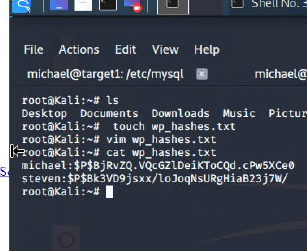


Hint was to look for MySql database password in /var/www/html/wordpress/wp-config.php



cd wordpress

cat wp-config.php



* + **flag2.txt:**

In the /var/[www.html](http://www.html)



Mysql commands

$ show database;

$ use wordpress;

$ show tables;

$ select \* from wp\_posts;

- `flag3`

Started just looking into every single table on mysql using the wordpress database

Flag3 ended up being displayed when typing “select \* from wp\_users”

Flag3{afc01ab56b50591e7dccf93122770cd2}

-’flag4’

Started just looking into every single table on mysql using the wordpress database

Flag3 ended up being displayed when typing “select \* from wp\_users”

flag4{715dea6c055b9fe3337544932f2941ce}

Found Steven’s password using John the ripper

