# Red Team: Summary of Operations

## Table of Contents

- Exposed Services

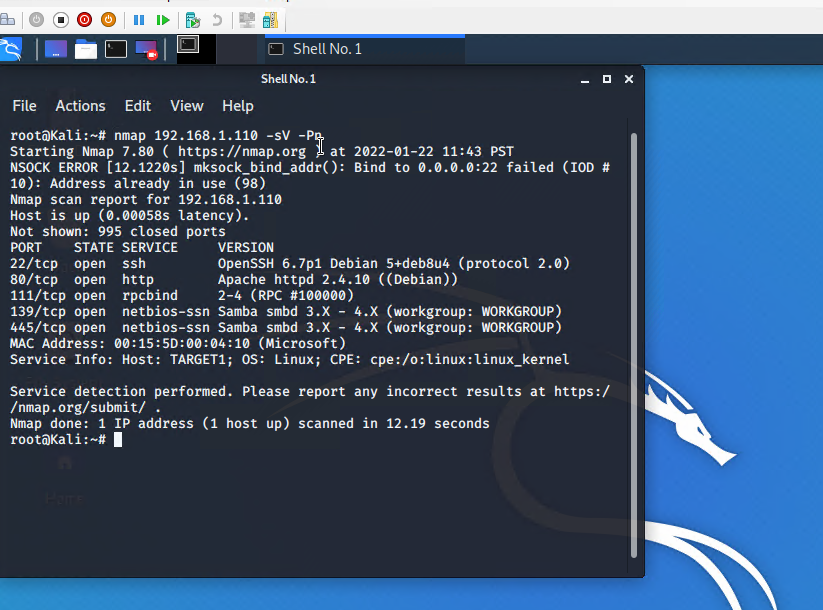
- Critical Vulnerabilities

- Exploitation

### Exposed Services

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

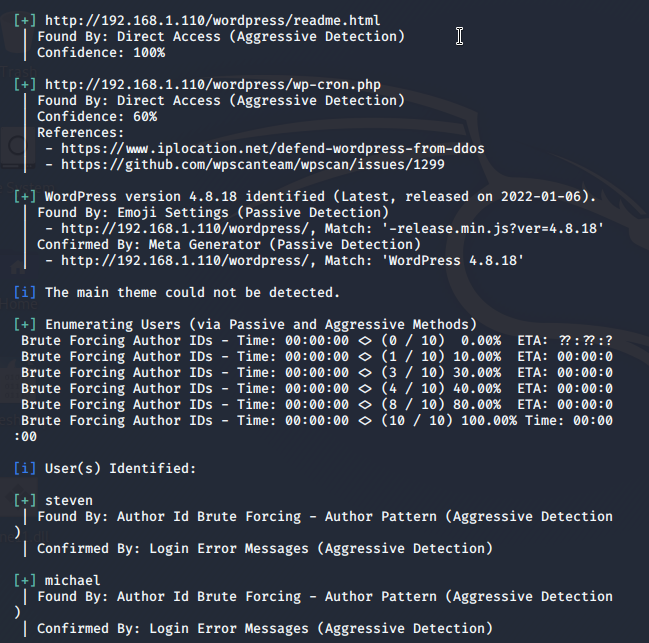
$ nmap 192.168.1.110 –sV –Pn

Target 1   
Critical: High  
Vulnerabilities: Port 22 is opened and it used for remote ssh connections, and port 80 is also opened for unsecured connection which can exposed unauthorized folders on the target environment.

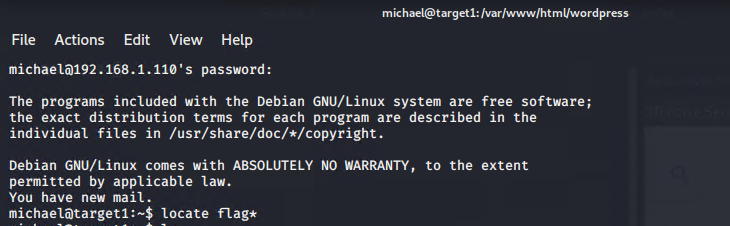
Enumerate the WordPress site against the target.

Target 2



  
  
Critical: High  
Vulnerabilities: provided user names on the target that can be potentially used for brute force.  
Simply having the username, the next step is to figure out the password.

There is a weak password for Michael.  
Target 3

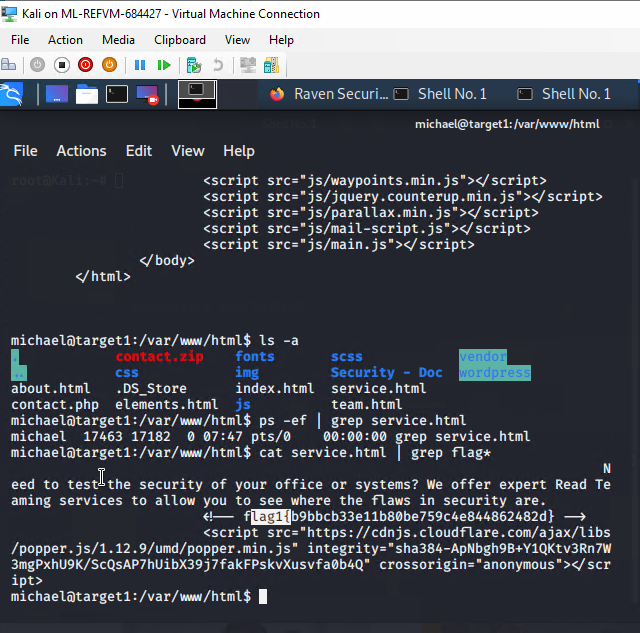


Critical: High   
Vulnerabilities: List of predictable and weak password for Michael through ssh from Kali machine (michael/michael). I was able to ssh to Michael’s home directory and navigate the filesystem.

**Exploitation**

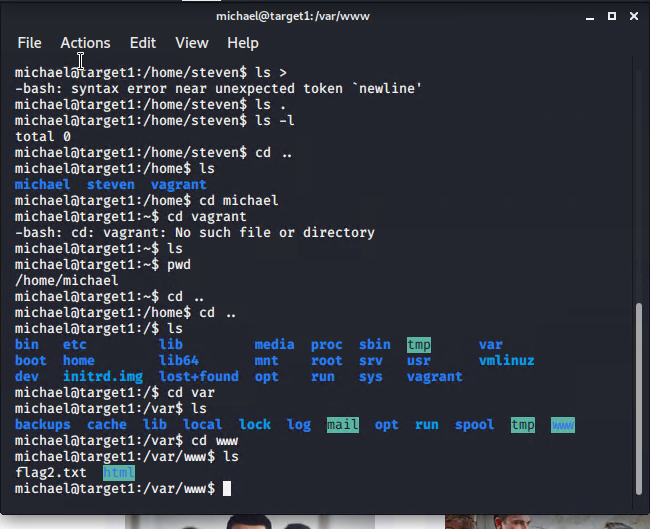
The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:

- Target 1

- 

- \*\*Exploit Used\*\*  
Exploring the folders to find flag1.txt

1) cd /var/www/html  
2) ls –a (to see the hidden files)  
3) cat service.html | grep flag\*  
4) the above screenshot illustrates the flag1 within the service.html file.



- \*\*Exploit Used\*\*

Exploring the folders to find flag2.txt

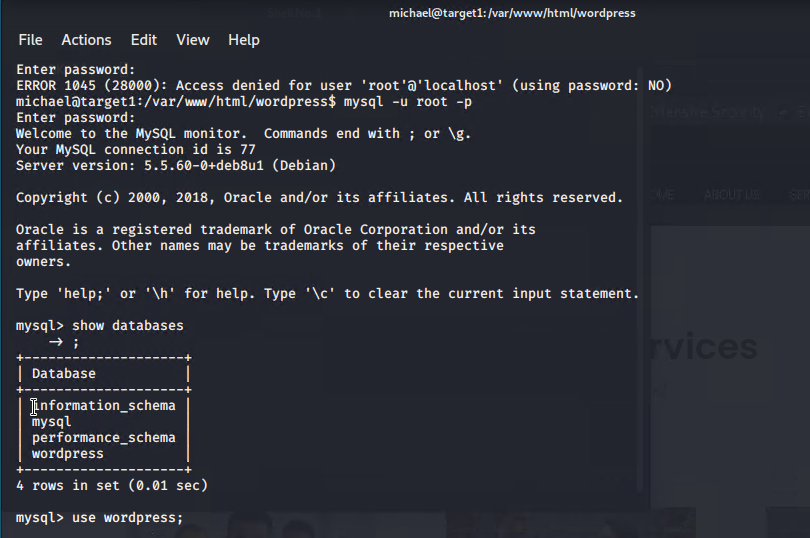
1) Cd .. (root folder)

2) ls (view the available directories on the root)

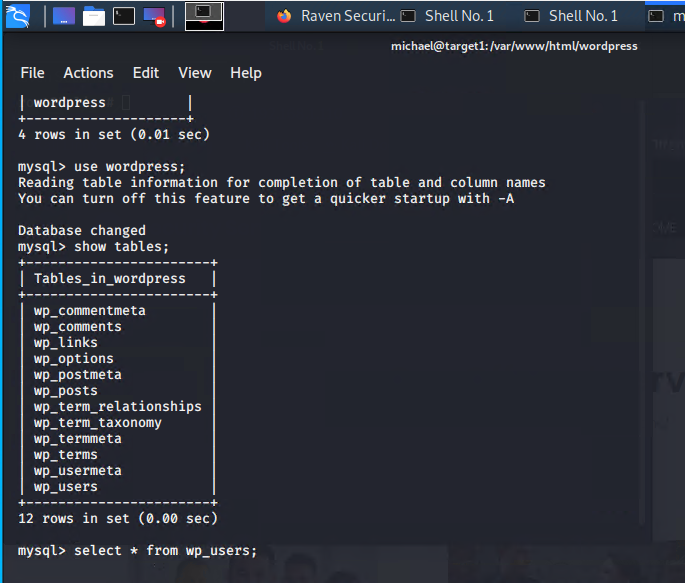
3) cd var/www

4) ls command showed flag2.txt

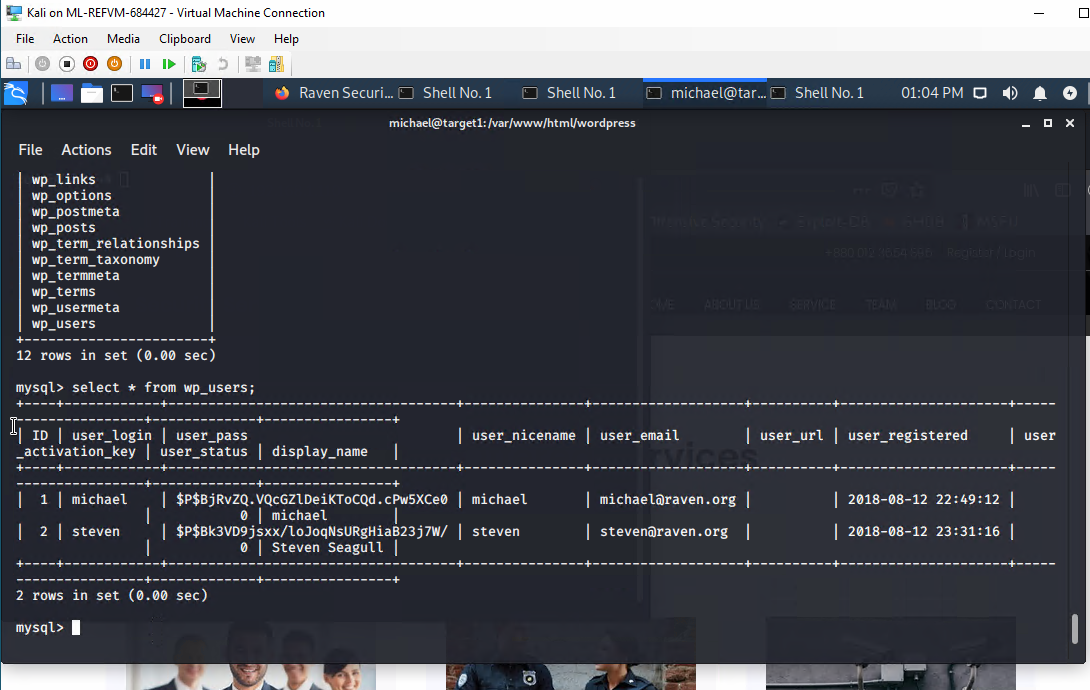
1) CD /var/www/html/wordpress and nano wp-config.php to get the user name and password for the mysql db

2) 

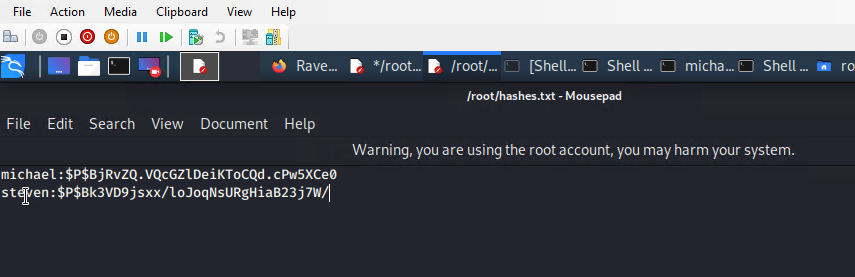
mysql – u root –p and   
entered the password retrieved from /var/www/html/wordpress/wp-config.php  
to get into the mysql database  
--show databases;

3) 

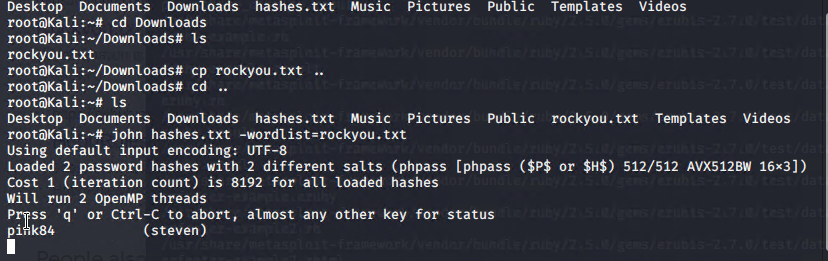
use wordpress database

4) 

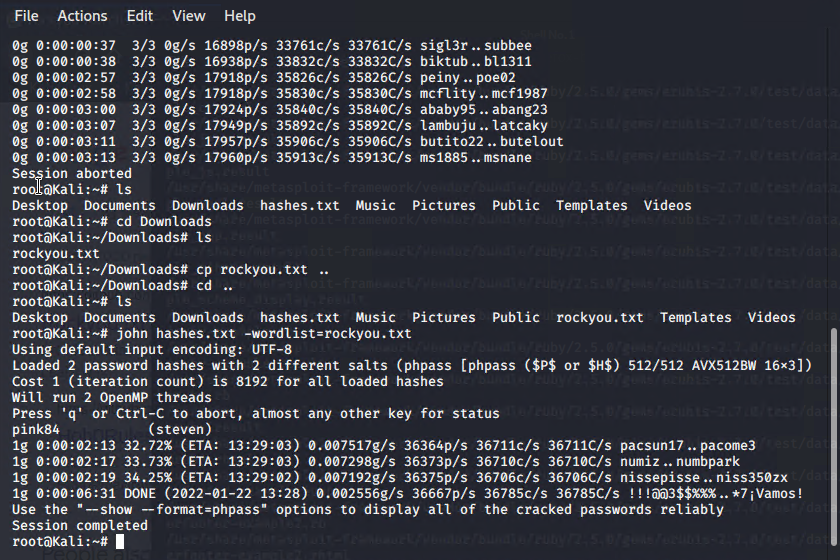
Executed select \* from wp\_users;

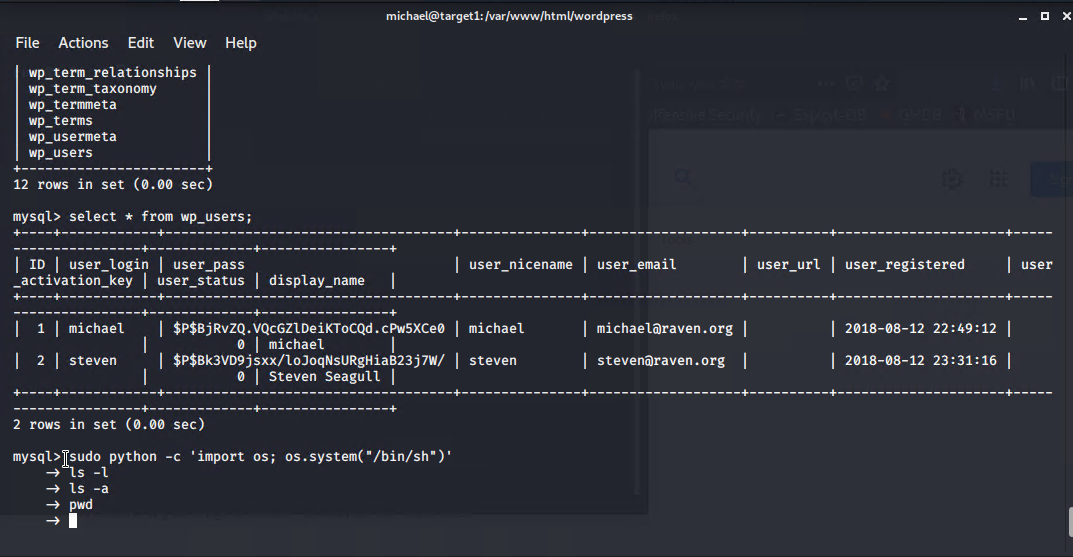
5)

Created the hash file on root directory, saved both hashes and users from the wp\_users table

6)  


Executed password brute forced for michael and steven - john hashes.txt –wordlist=rockyou.txt

7)   
8)



We escalated the privileges by using the following command:  
sudo python -c 'import os; os.system("/bin/sh")'