# **Offensive: Summary of Operations**

## **Table of Contents**

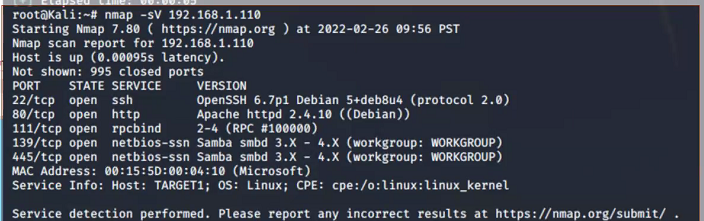
* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

nmap -sV 192.168.1.110

Output for Target 1:



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

* Target 1
  + List of Ports: 22, 80, 111, 139, 445
  + Exposed Services: ssh, http, rpcbind, netbios-ssn

The following vulnerabilities were identified on each target:

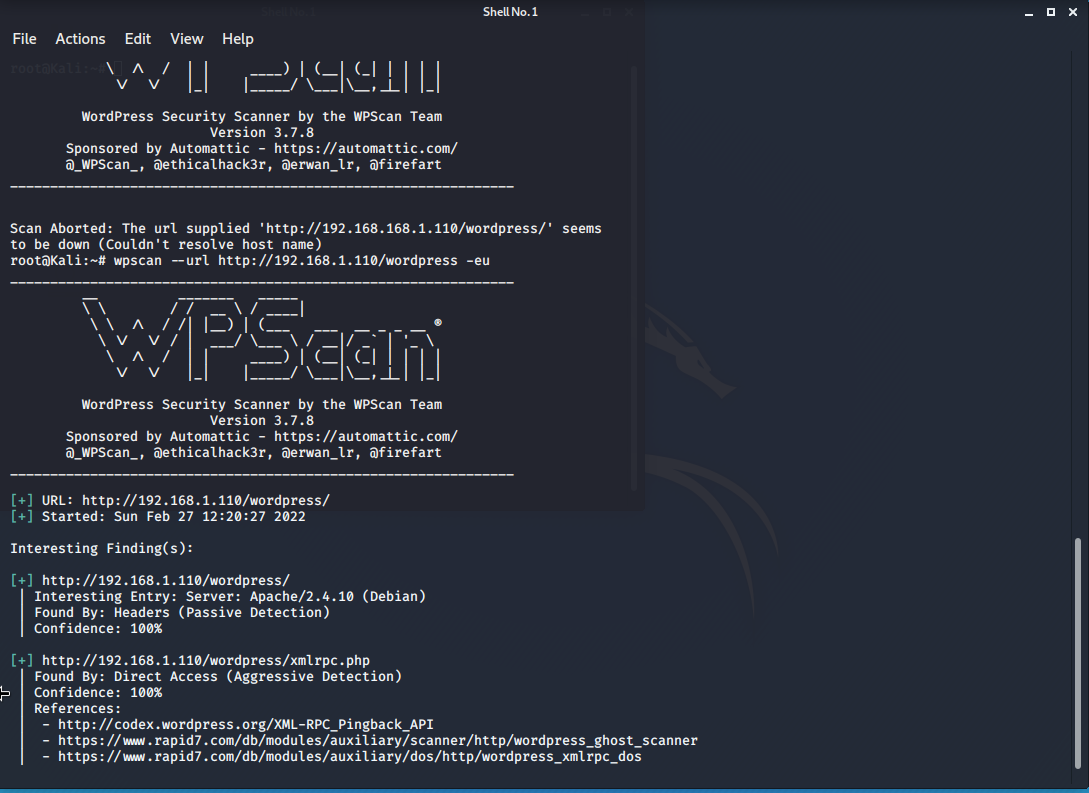
* Target 1

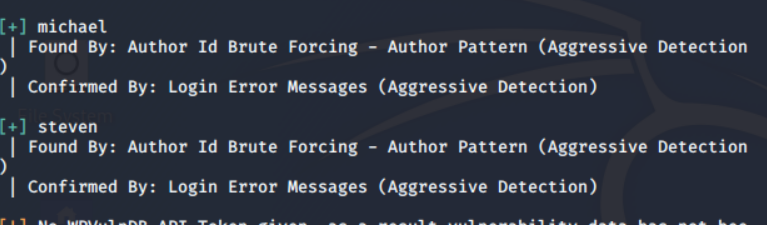
List of Critical Vulnerabilities:

* CVE-2021-44142 remote attackers with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.
* CVE-2017-8779(rpcbind) allows remote attackers to cause a denial of service (memory consumption with no subsequent free) via a crafted UDP packet to port 111, aka rpcbomb.

### **Exploitation**

*Wpscan –url* [*http://192.168.1.110/wordpress*](http://192.168.1.110/wordpress) *-eu*

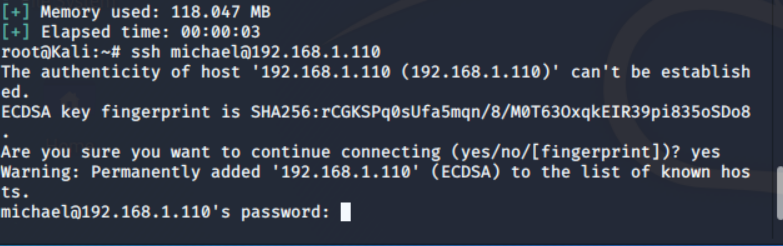
**

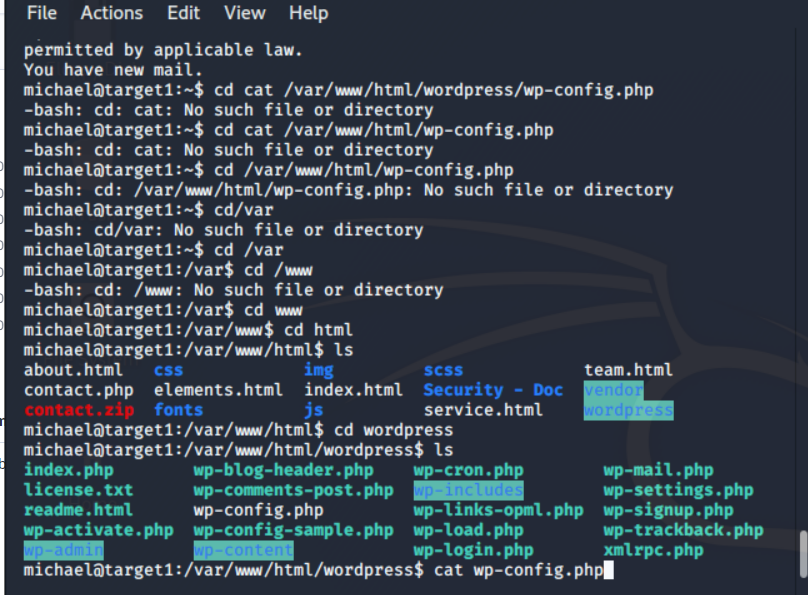
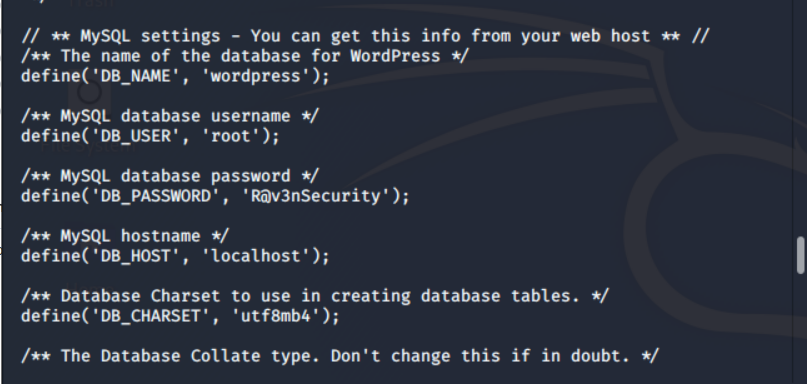
**

*Password: michael*

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

* Target 1
  + SSH into Micheals account*:*
* **Exploit Used**
  + *Weak password. Used Micheal password to log in which was micheal.*
  + *Include the command run: ssh michael@192.168.1.110*

**

* *Once logged in as Michael we navigated to /var/www/html/wordpress directory.*
* **
* *Then we did: cat wp-config.php*
* **

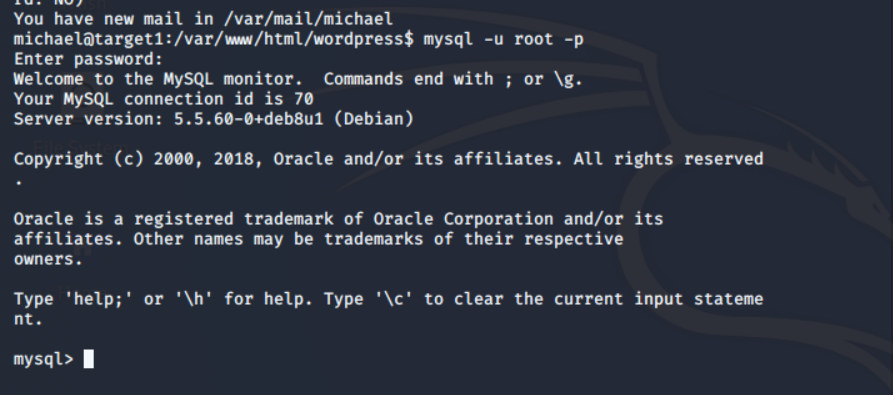
*MySQL login*

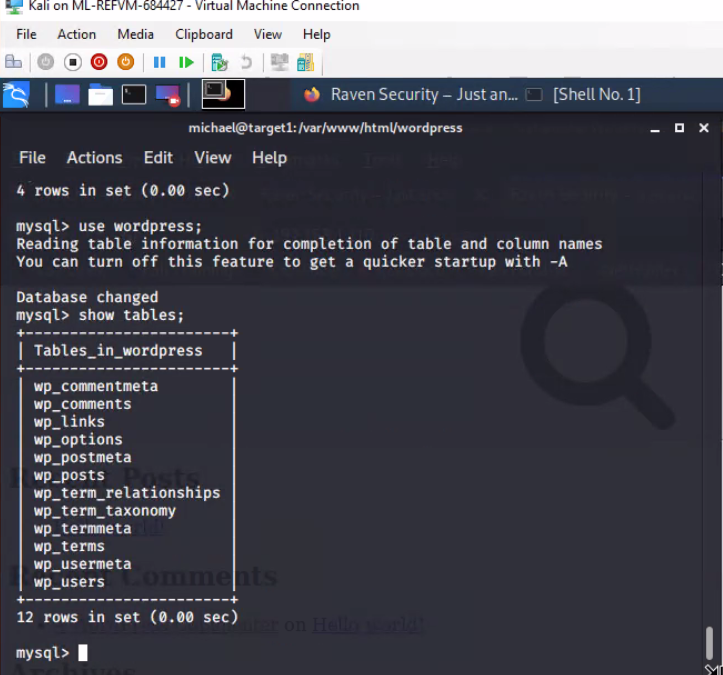
**Exploit Used**

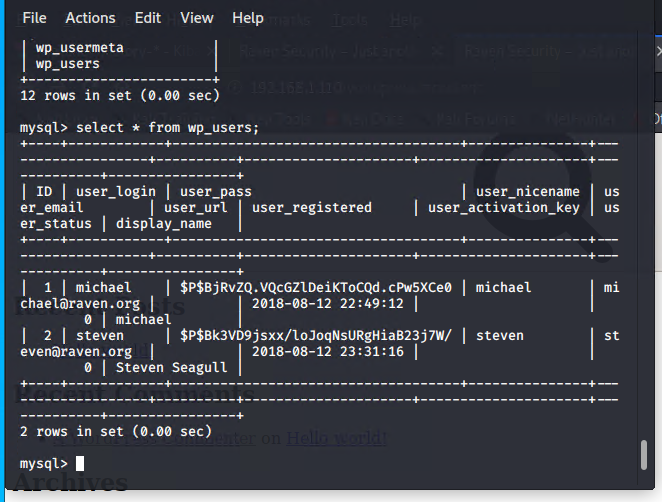
*Used Michael credentials to access wp-config.php file.*

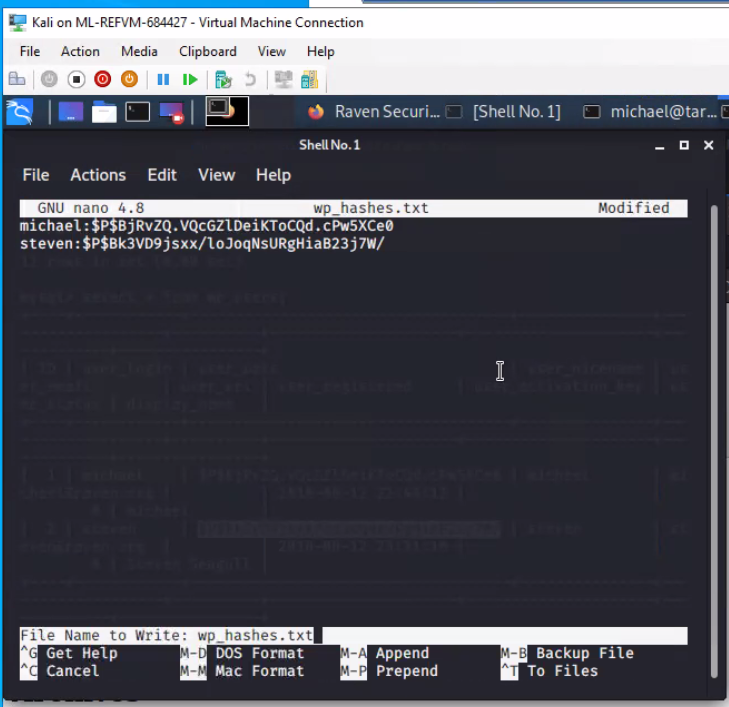
*Command: mysql -u root -p*

* + - * + *user: root password:R@v3Security*

**

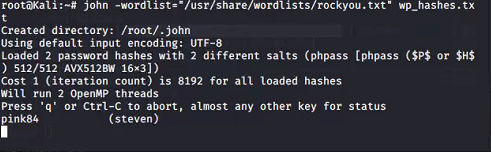
**

* *Command: select \* from wp\_users;*
* **
* *Next we made a file with the names and hashes of Michael and Steven. File name is wp\_hashes.txt*

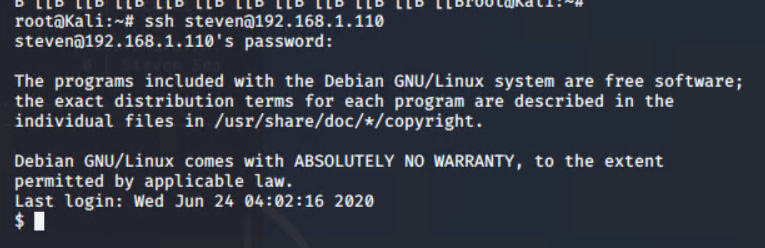


* *Next we ran the file through John the Ripper.*

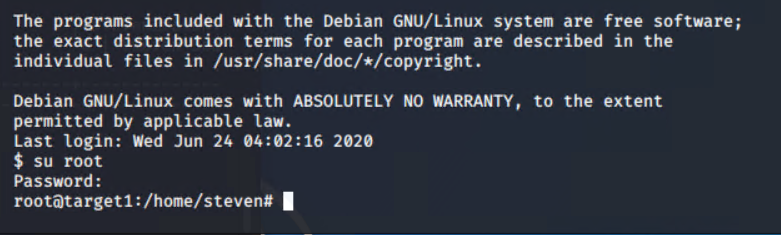
*Command: john -wordlist=”/usr/share/wordlists/rockyou.txt” wp\_hashes.txt*

**

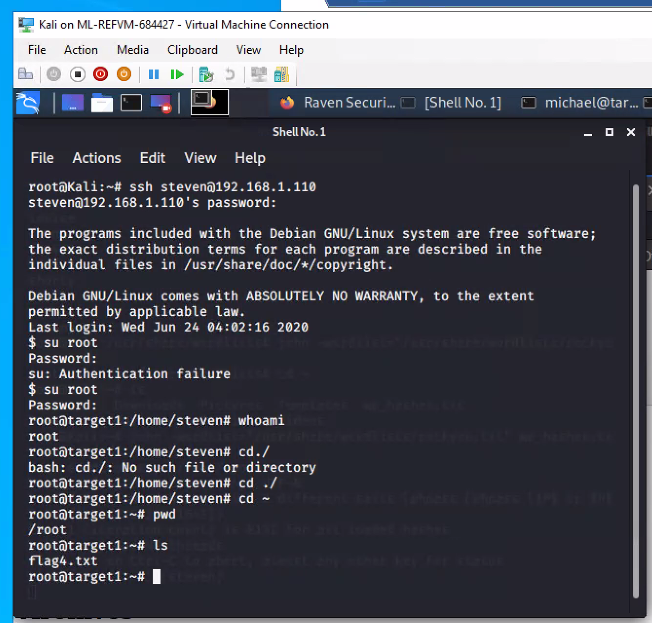
* *Next we step was to ssh steven@192.168.1.110.*

**

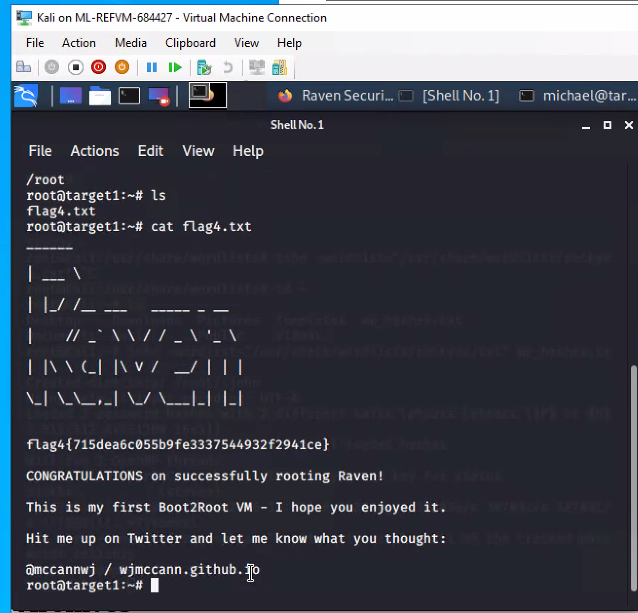
* *The Next step was to escalate to root. Command: su root Password: toor*

**

* *Then we cd ~ to the home directory.*



* Next we cat the flag4.txt file.

**