# **Red Team: Summary of Operations**

## **Table of Contents**

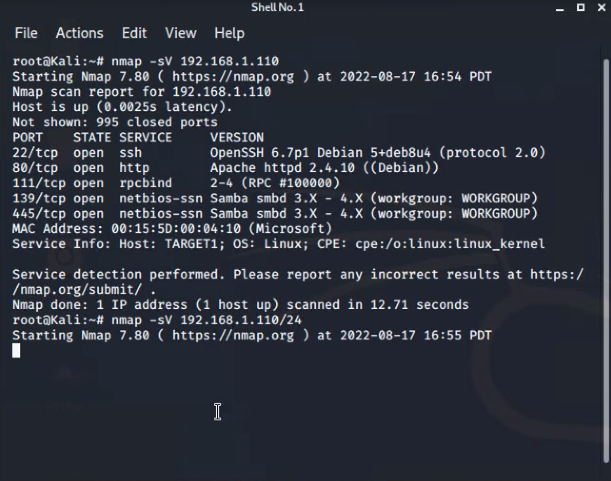
* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

First identifying the IP address from Kali Linux can be done using ifconfig.

The results of that shows that the IP of the Kali machine is 192.168.1.110

After this, an nmap scan using the following command: nmap -sV 192.168.1.110



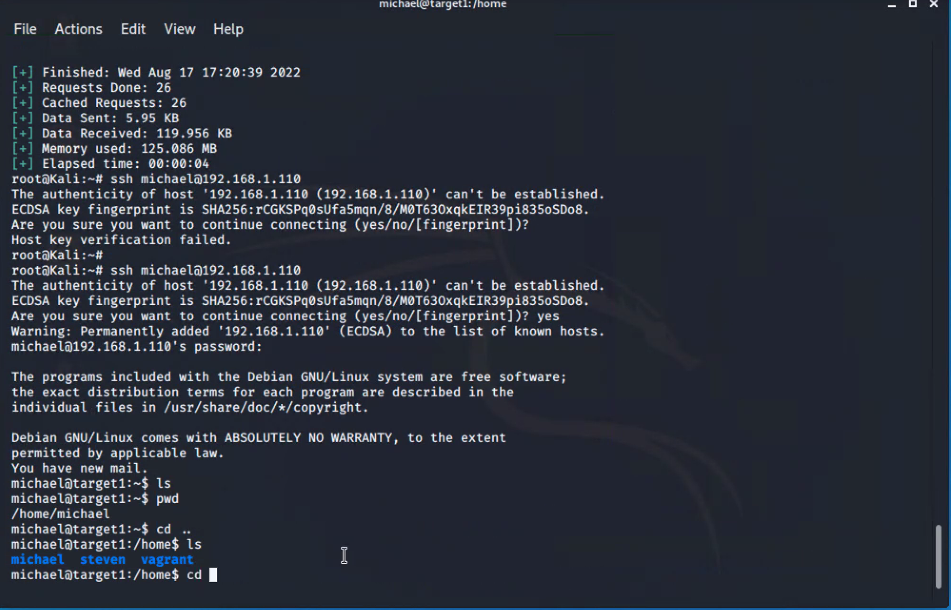
This scan identifies the services below as potential points of entry:

Target 1

* Port 22 / TCP Open SSH
* Port 80 / TCP Open HTTP
* Port 111 / TCP Open RPCBind
* Port 139 / TCP Open netbios-ssn Samba
* Port 445 / TCP Open netbios-ssn Samba

The following vulnerabilities were identified on each target:

* Target 1
  + Having weak password credentials
  + Lack of proper user privilege settings. Users can escalate and misuse their privileges.



### **Exploitation**

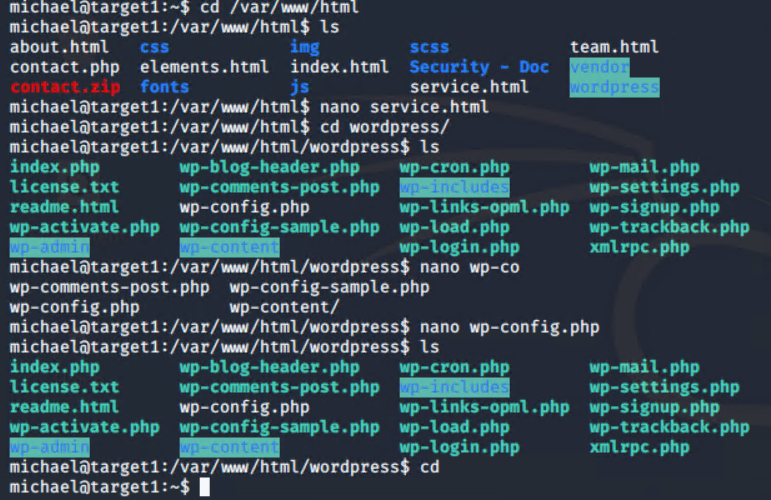
*The Red Team was able to penetrate Target 1 and retrieve the following confidential data:*

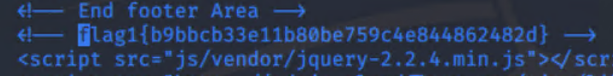
*●Flag 1: b9bbcb33ellb80be759c4e844862482d*

*●SSH as Michael and using Directory traversal to look through files*

*Commands include:*

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

**

**

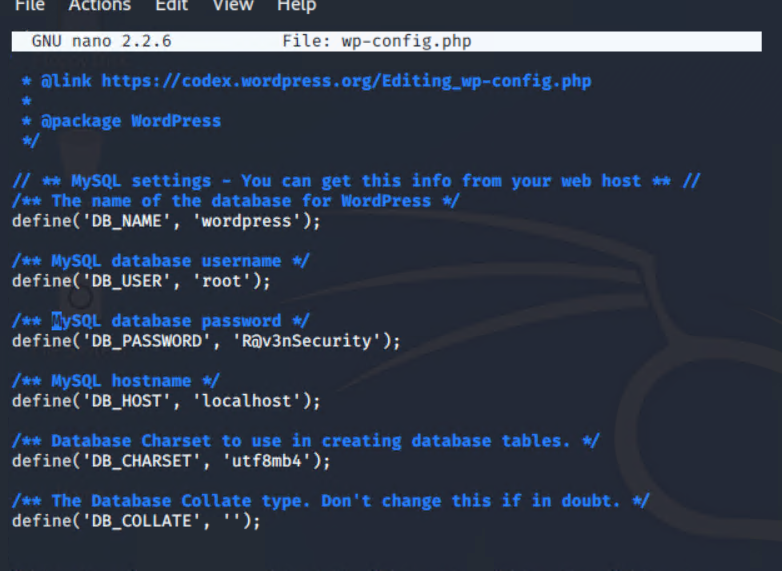
* + - **Exploit Used**

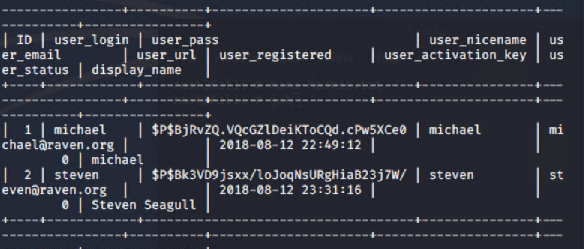
**The Red Team was able to penetrate Target 1 and retrieve the following confidential data:**

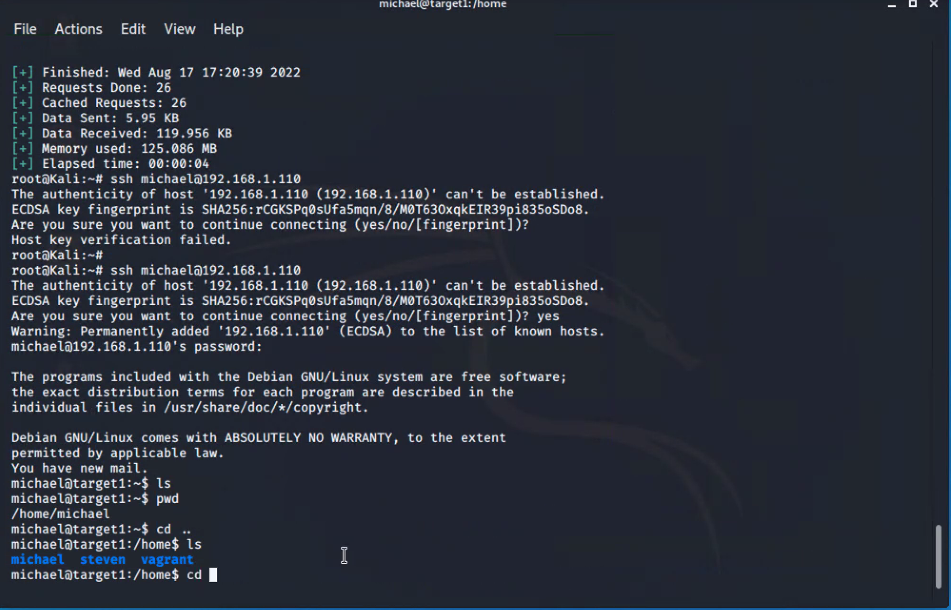
* **MySql Database password for wordpress**
* **Wordpress hashes for both Michael & Stevens password hashes**
* **SSH as Michael and using Directory traversal to look through files**
* **Flag 2:fc3fd58dcdad9ab23faca6e9a3e581c**

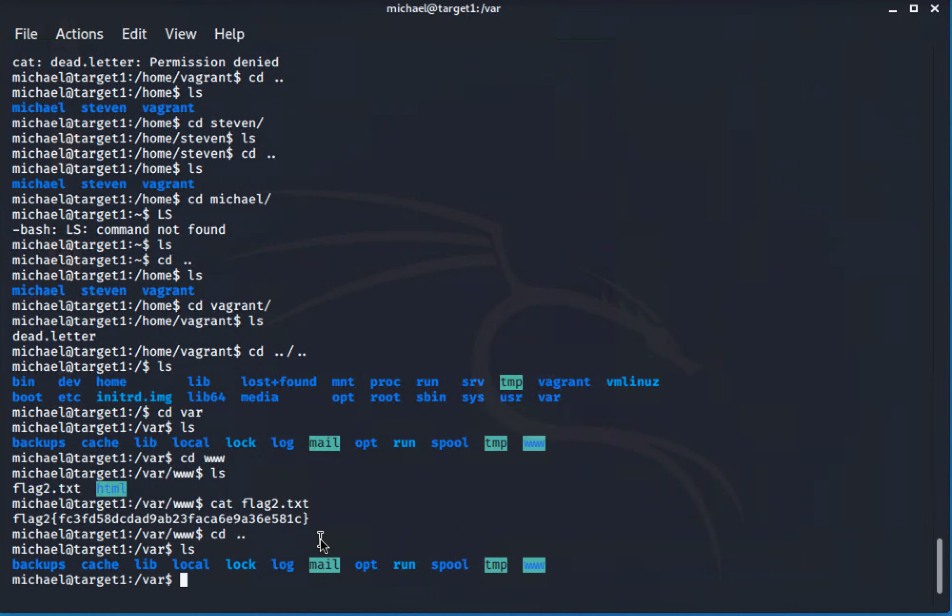
**Commands include:**

* **ssh@192.168.1.110**
* **pw: pink84**
* **cd var/www**
* **Cat flag2.txt**

****

****

****

****