# Red Team: Summary of Operations

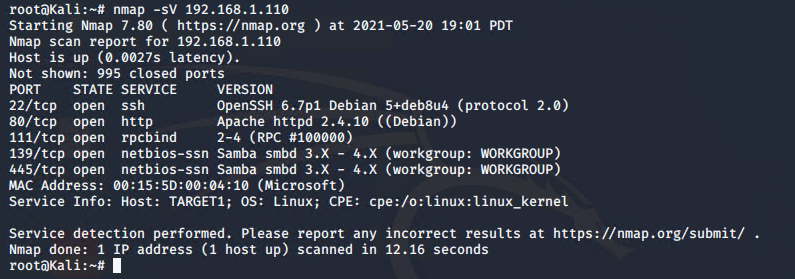
## 

## Table of Contents

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### Exposed Services

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



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

**Target 1**

1. Ssh (port 22)
2. Http (port 80)
3. Rpcbind (port 111)
4. Netbios-ssn Samba (ports 139 & 445)

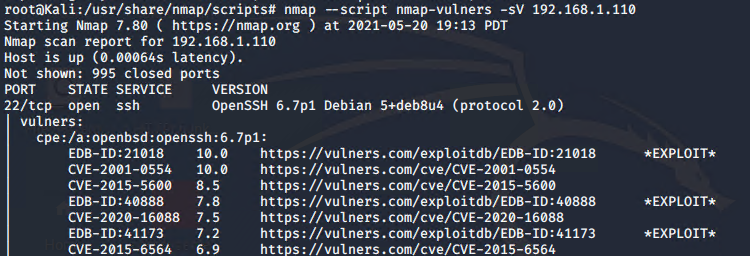
### Critical Vulnerabilities

The following vulnerabilities were identified on Target1:

**Target 1**

The following are the most critical CVE’s identified using nmap to scan for vulnerabilities against target 1

1. CVE-2001-0554
2. CVE 2015-5600
3. CVE 2020-16088



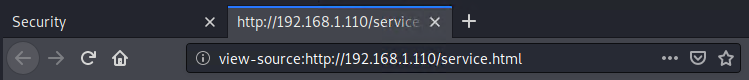
Exploitation

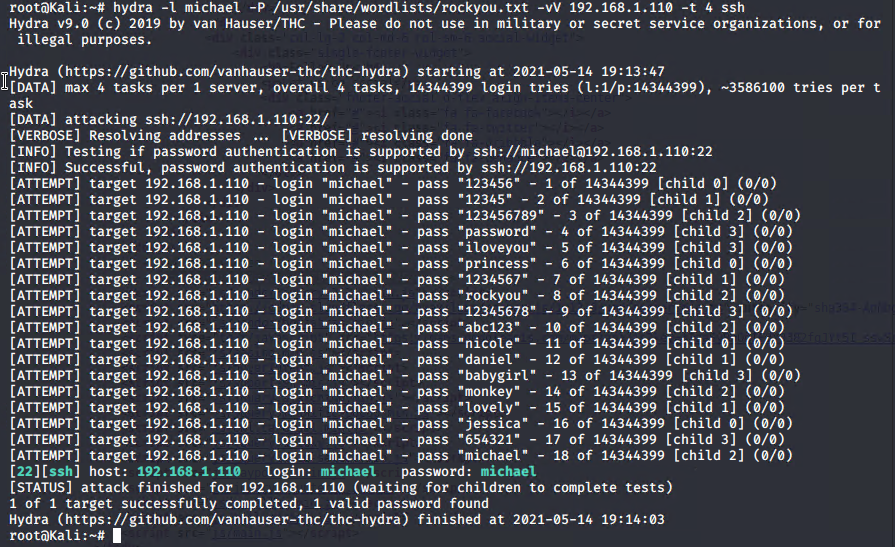
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

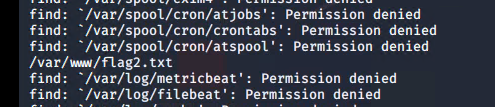
**Target 1**

* **flag1.txt:** 
* Note: flag1 can be found by either viewing source code on the web page (service.html - line 262) or by opening the file in /var/www/html/service.html.

“nano /var/www/html/service.html”

* Exploit Used
  + Exploit used was the fact that the web page source code was not protected and included the flag information. Also the password policy obviously allows the use of weak passwords (michael:michael) making it easy to get a shell on the target machine using ssh.
  + 
* flag2.txt: 
* Exploit Used
  + Exploit was the weak password policy allowing michael to specify a username and password both the same and easy to guess (michael:michael).
  + The password was cracked using Hydra as follows:-

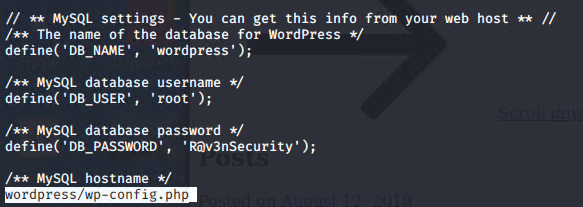


* The flag was found using the command
  + **“find / flag\*”**
  + ****

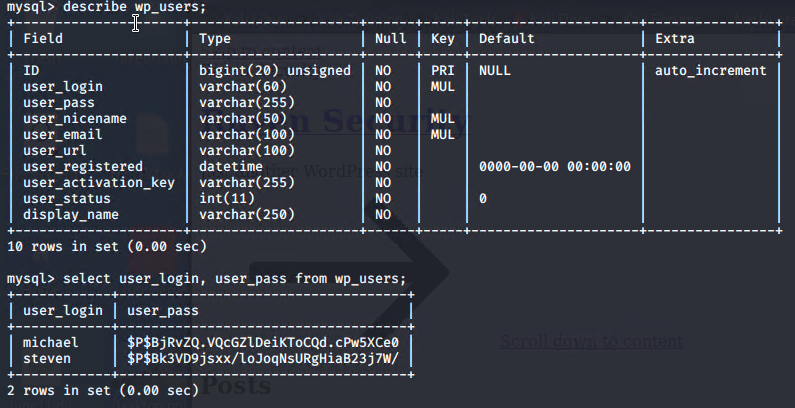
Flag3.txt : 

* Exploit used : Providing cleartext user passwords combinations for access to the mySql database
* Flag 3 was found by first running
  + “Less /var/www/html/wordpress/wp-config.php

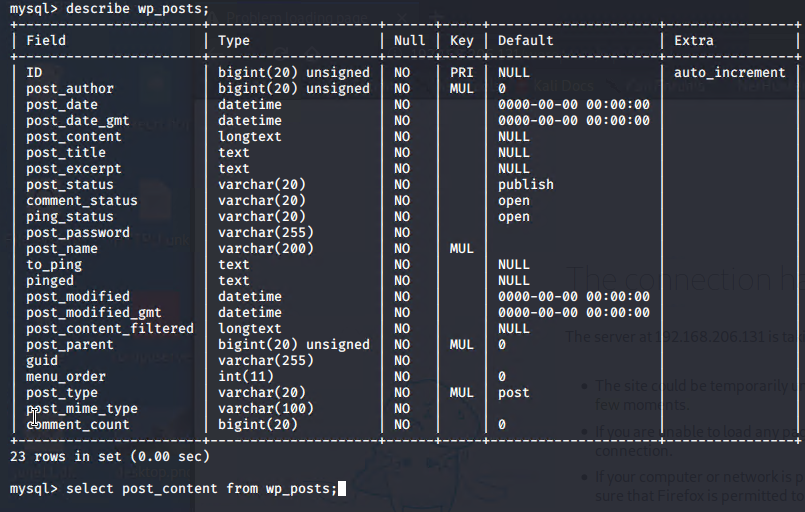
This was able to provide the SQL database password

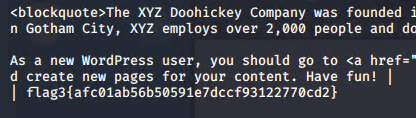


* After logging in to mySQL we were able to access the wordpress database and all its tables. Two tables were interesting.
  + Wp\_users
  + Wp\_posts
* Wp\_users gave us the hash for both steven and michael



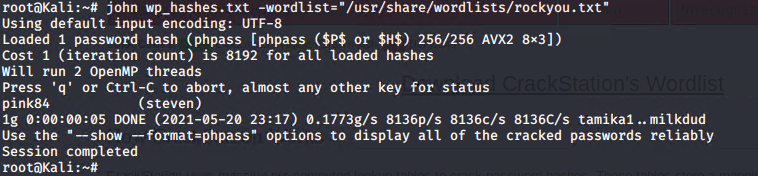
* Wp\_posts gave us flag 3



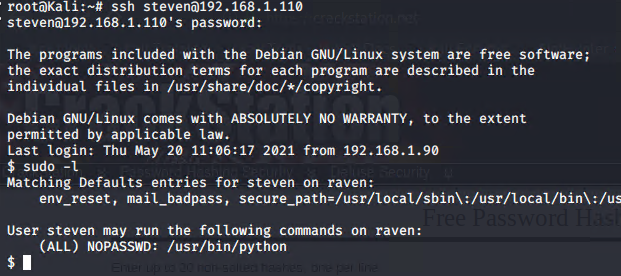


Flag 4:

* Exploit Used: Poor password policy meant that Stevens password was easy to crack using John



* By logging in as Steven via ssh we were able to use a Python script to gain root access and flag 4



* Remaining commands below:

