**Red Team: Summary of Operations**

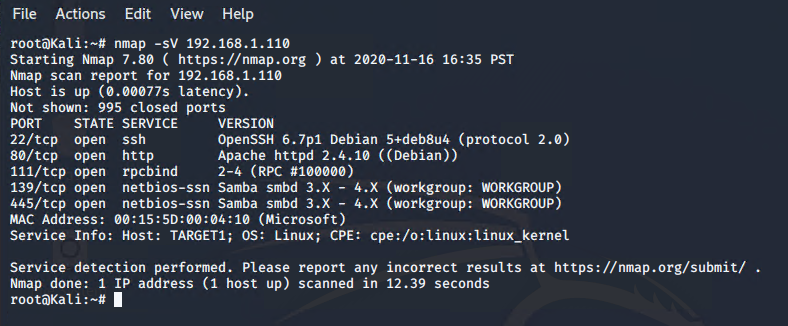
**Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

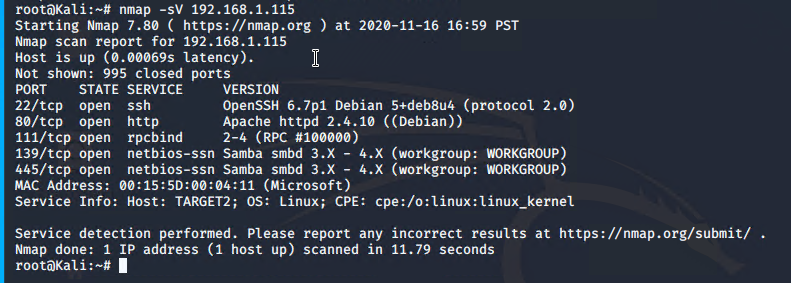
**Exposed Services:**

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

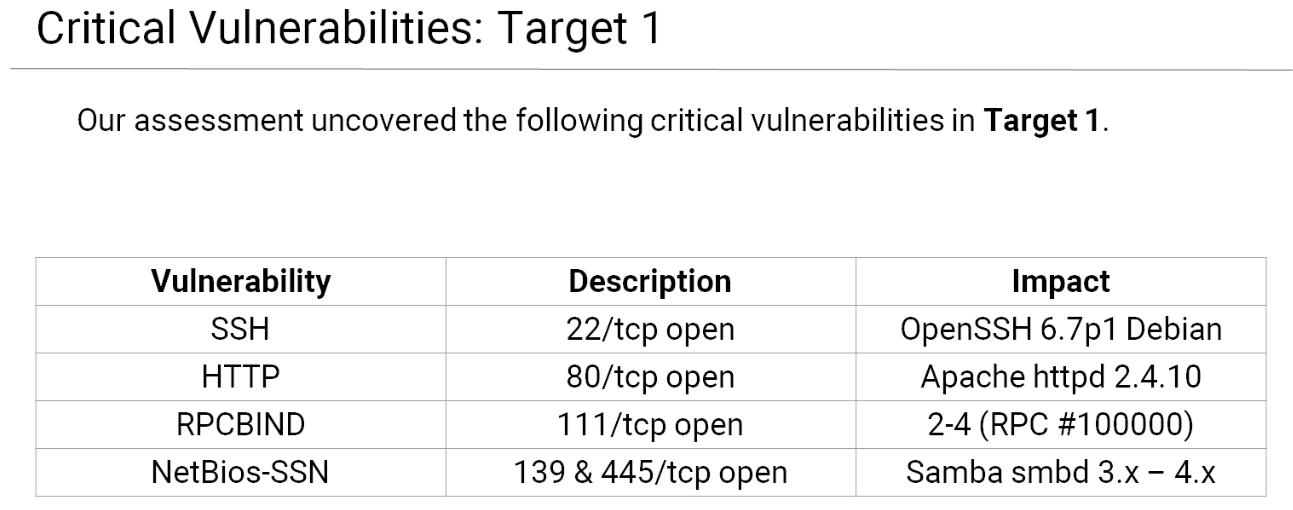
**$ nmap -sV 192.168.1.110 for Target 1**

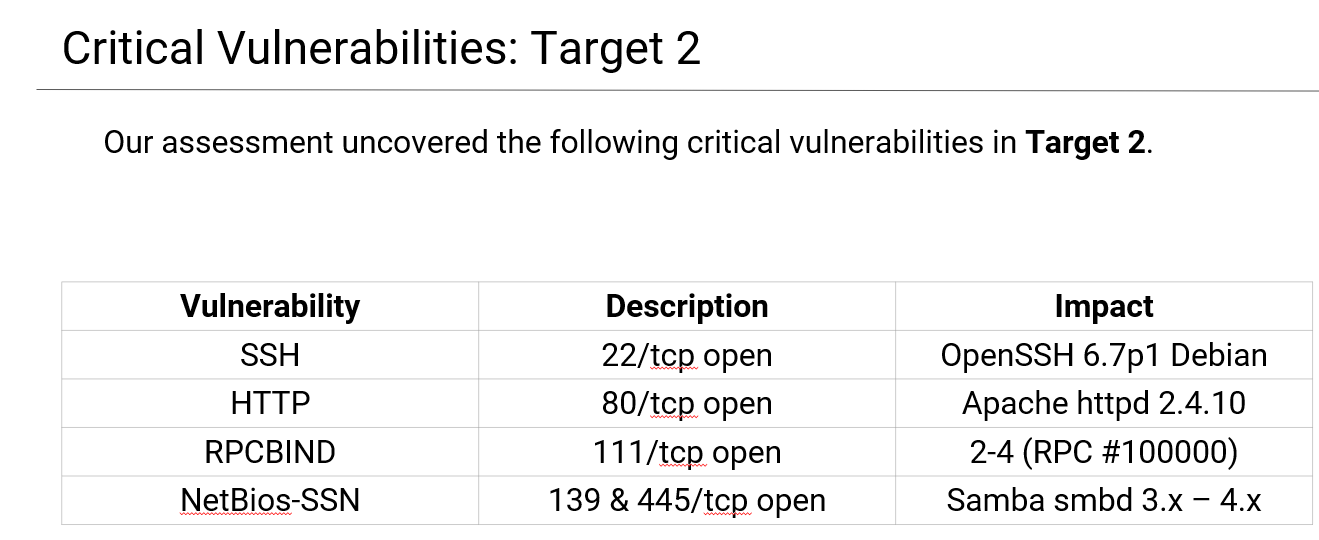


**$ nmap -sV 192.168.1.115 for Target 2**



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





**Critical Vulnerabilities**

Fill out the list below. Include severity, and CVE numbers, if possible.\_

The following vulnerabilities were identified on each target:

Target 1

* Port 22 is open: allows for the ability to ssh into a remote machine with discovered credentials
* Port 80 is open and running an older version of Apache: Allows physical access to the http / web server and manipulation of web content such as cross scripting.

Target 2

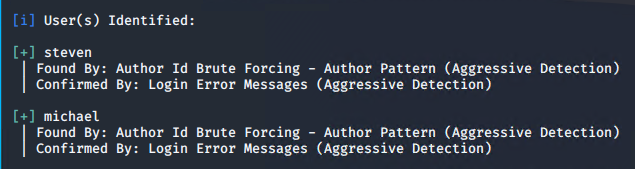
* Port 22 is open: allows for the ability to ssh into a remote machine with discovered credentials
* Port 80 is open and running an older version of Apache: Allows physical access to the http / web server and manipulation of web content such as cross scripting.

**Exploitation**

Fill out the details below. Include screenshots where possible

$ wpscan –url: <http://192.168.1.110/wordpress> --enumerate u

TARGET 1 Users:



TARGET 2 Users:

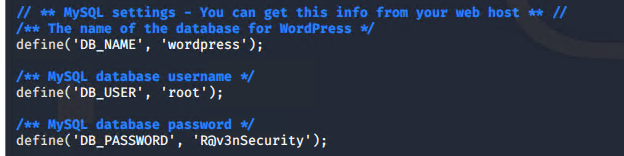


**SSH exploit on Target1**

SSH via port 22:

$ ssh [michael@192.168.1.110](mailto:michael@192.168.1.110)

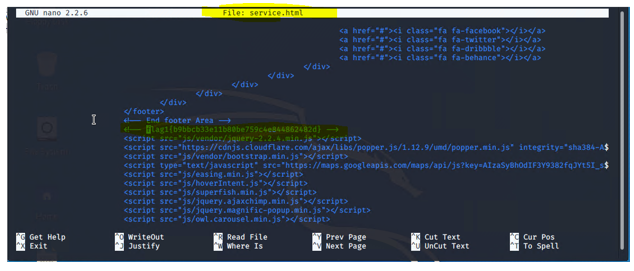
Located the wp-config.php file to reveal the user ID and password for mysql via Michael’s login:



The Red Team was able to penetrate both `Target 1` and `Target 2`, and retrieve the following confidential data:

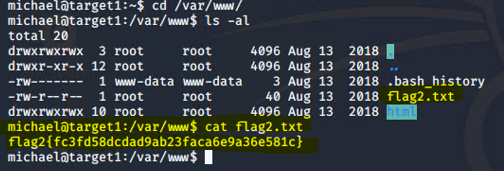
**Target 1 – Flags Found**

**Flag 1:** Found in the service.html file under Michael’s login and in the var/www/html/ directory. Performed the nano command on service.html and performed a find to locate flag one (see screenshot below).



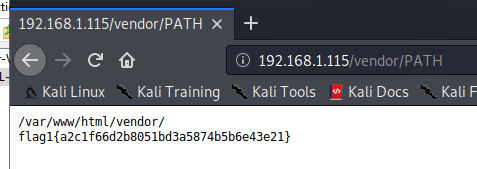
**Flag 2:** Located under Michael’s user account by using the following commands:

* Command: locate -I flag to find flag2.txt in the /var/www/ directory
* Command: cd /var/www/ to change directories
* Command: ls -al to reveal any hidden files or directories as well
* Command: cat flag2.txt to reveal the following hash stored in that file.



**Target 2 – Flags Found**

**FLAG 1 on Target 2:**



**FLAG 2 on Target 2**:

Using the shell you've opened on Target 2, find a flag in /var/www

