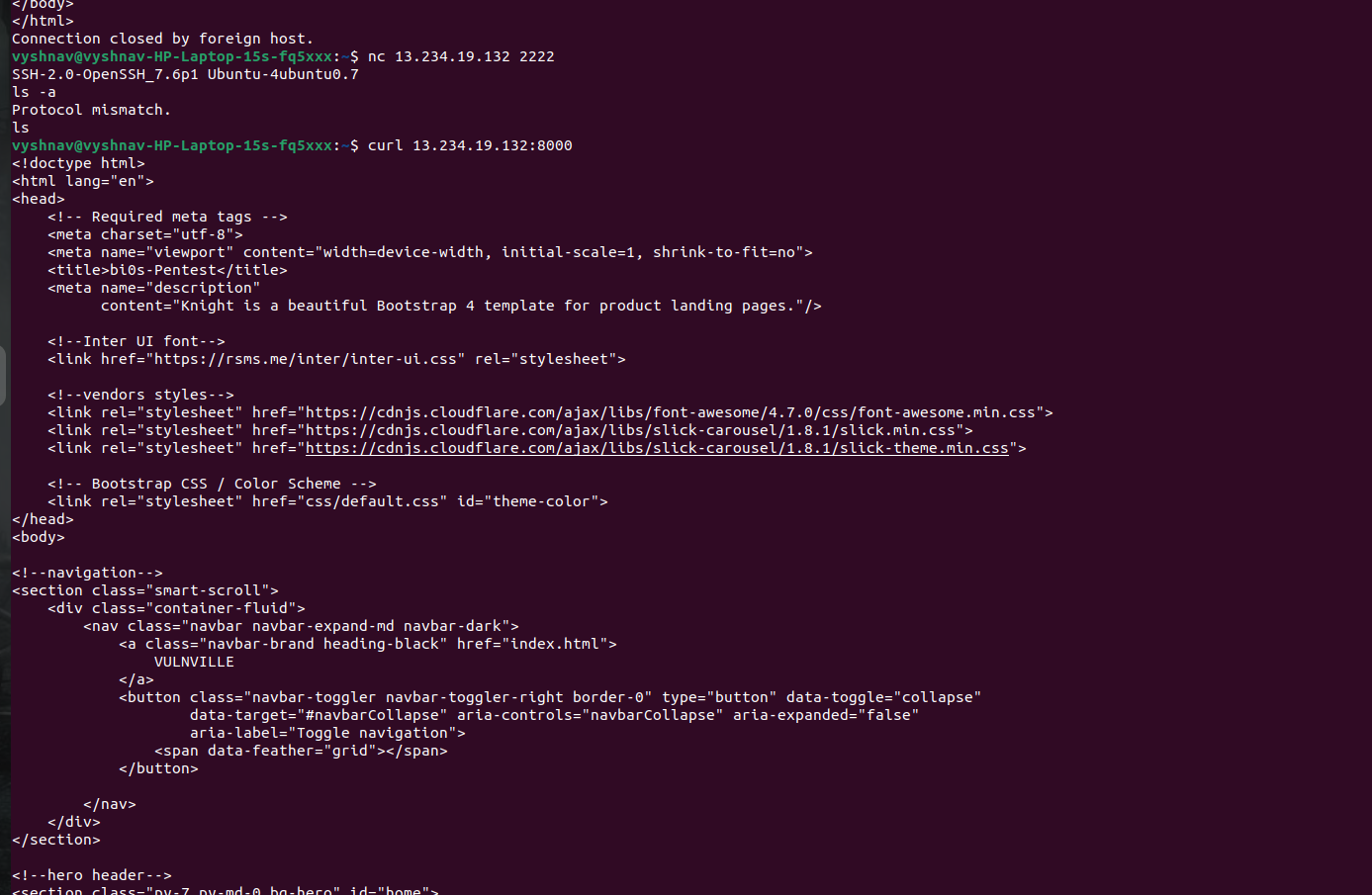
**STATUS UPDATE**

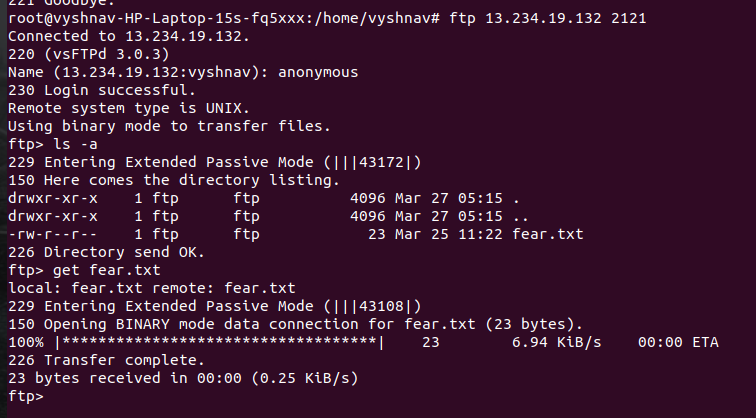
**BI0S PENTEST**

Found all the open ports and its services for the ip-address using ‘nmap’ command.

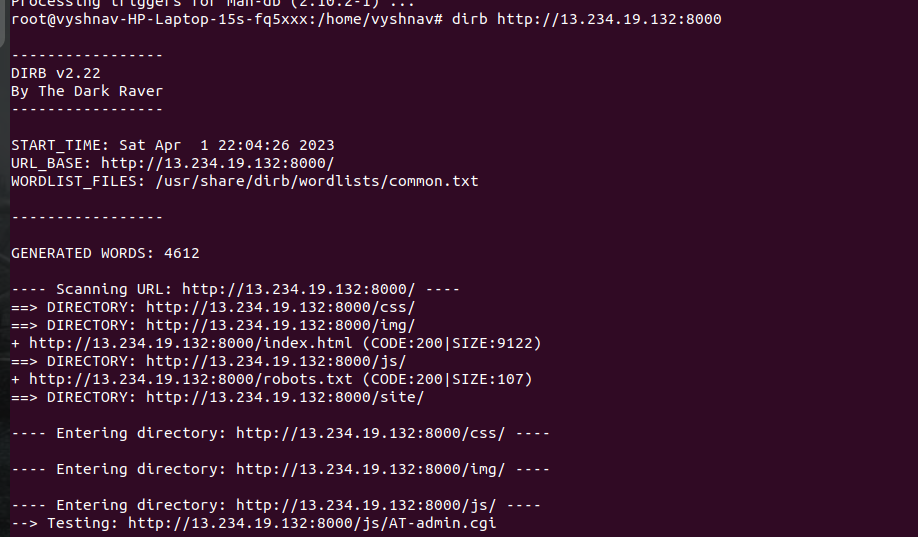


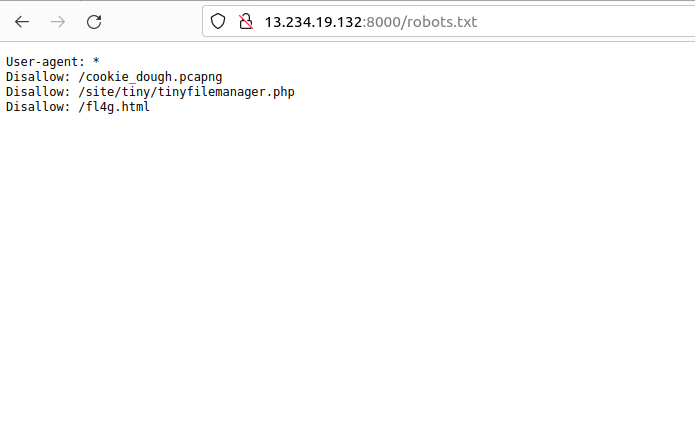
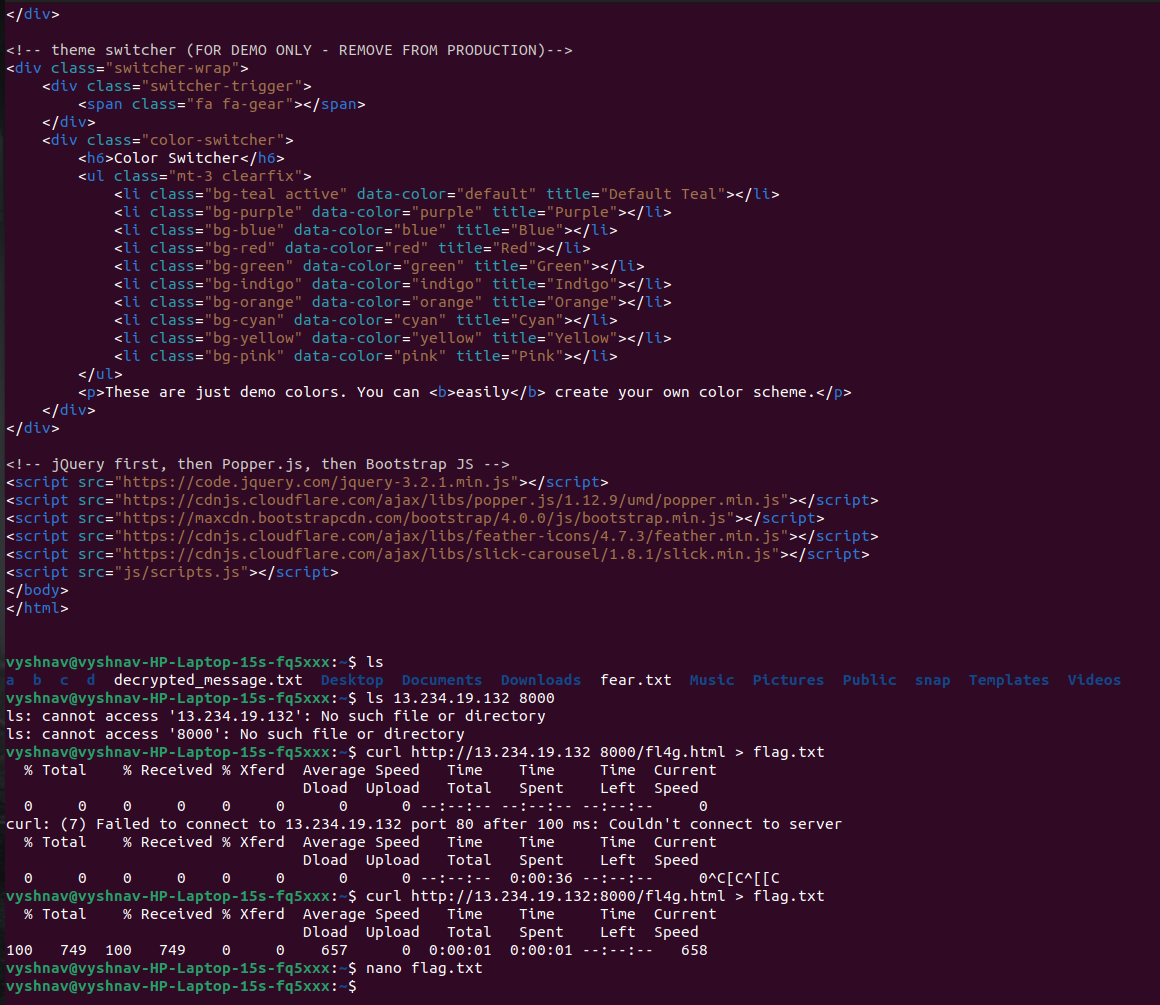


Tried connecting to the http port 8000 using curl command and found the websites source code. Didn't find any flag in it.



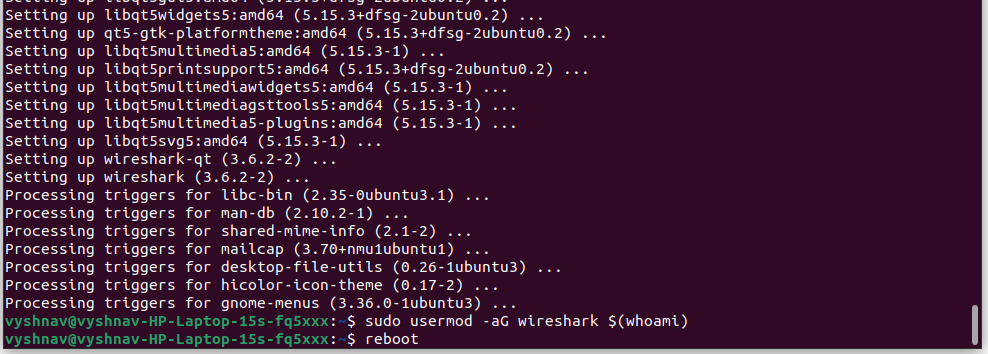
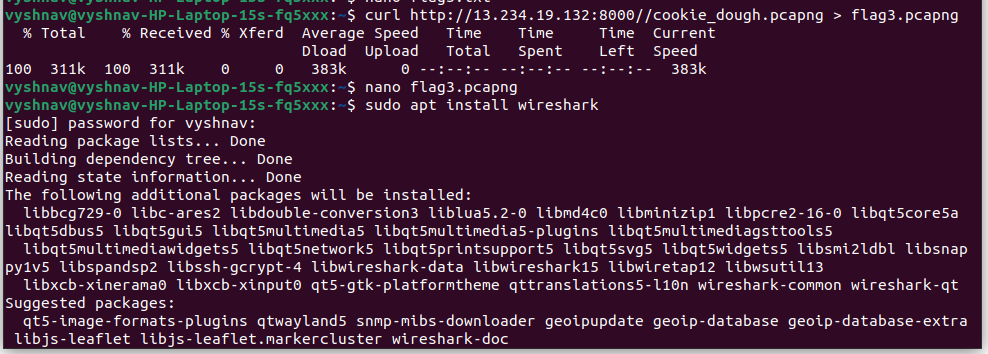
After that tried connecting to the ftp port 2121 using the command for connecting to the port, then giving name as ‘anonymous’ the login was successful and found a file fear.txt in it. Then using the get command transferred the file. Then found the flag in the required format after opening the file.

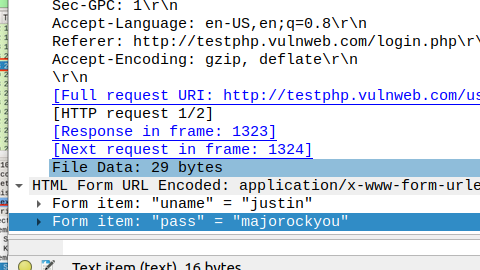


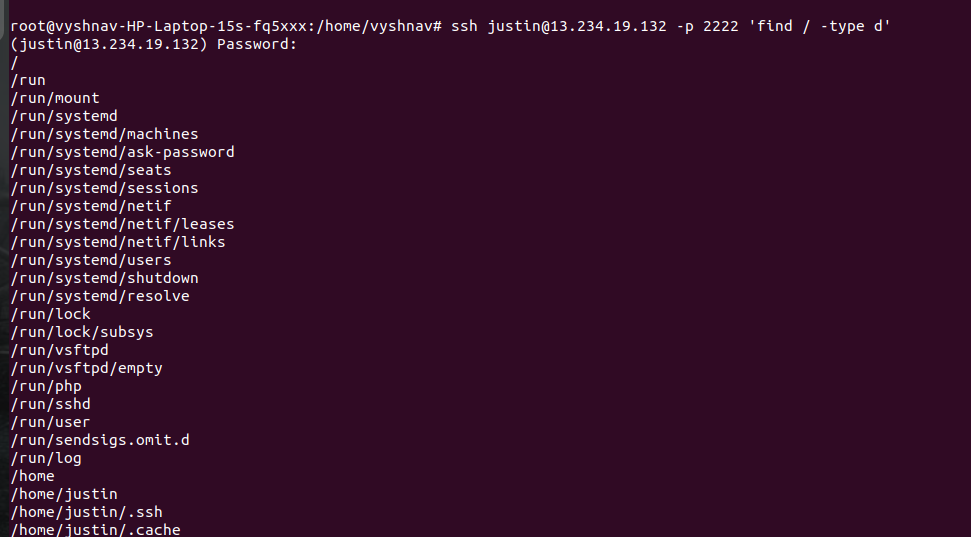
After referring to a github-repo of a similar task, found the ‘drib’ command for scanning all the directories and found all the hidden files in it for port 8000. Opened the /robot.txt file and found  

that it contained a fl4g.html file. 

After downloading and opening the file using ‘nano’ command found the flag.

While trying to connect to the ssh port 2222, first it was showing errors and then it was asking for password. So, the next task was to find out what it was. Got to know that it could be found in the .pcapng file. So, downloaded it and opened, but it was in an encoded format and didn’t understand anything. Then after referring to internet found that it could be found using an app called wireshark. So, I installed it.

Then after watching a tutorial video on using the app to find the password, found both the username and passwd.

Then tried connecting to the ssh port first the connection was not established. But, then trying again it showed all the file in it and did not establish a connection. Found that it happened because I sued the find comman in it.

Then after using the correct command, the connection was established. The using ‘ls’ command found all the files in the system. Then using ‘cat’ command I opened a read.txt file and found the flag.