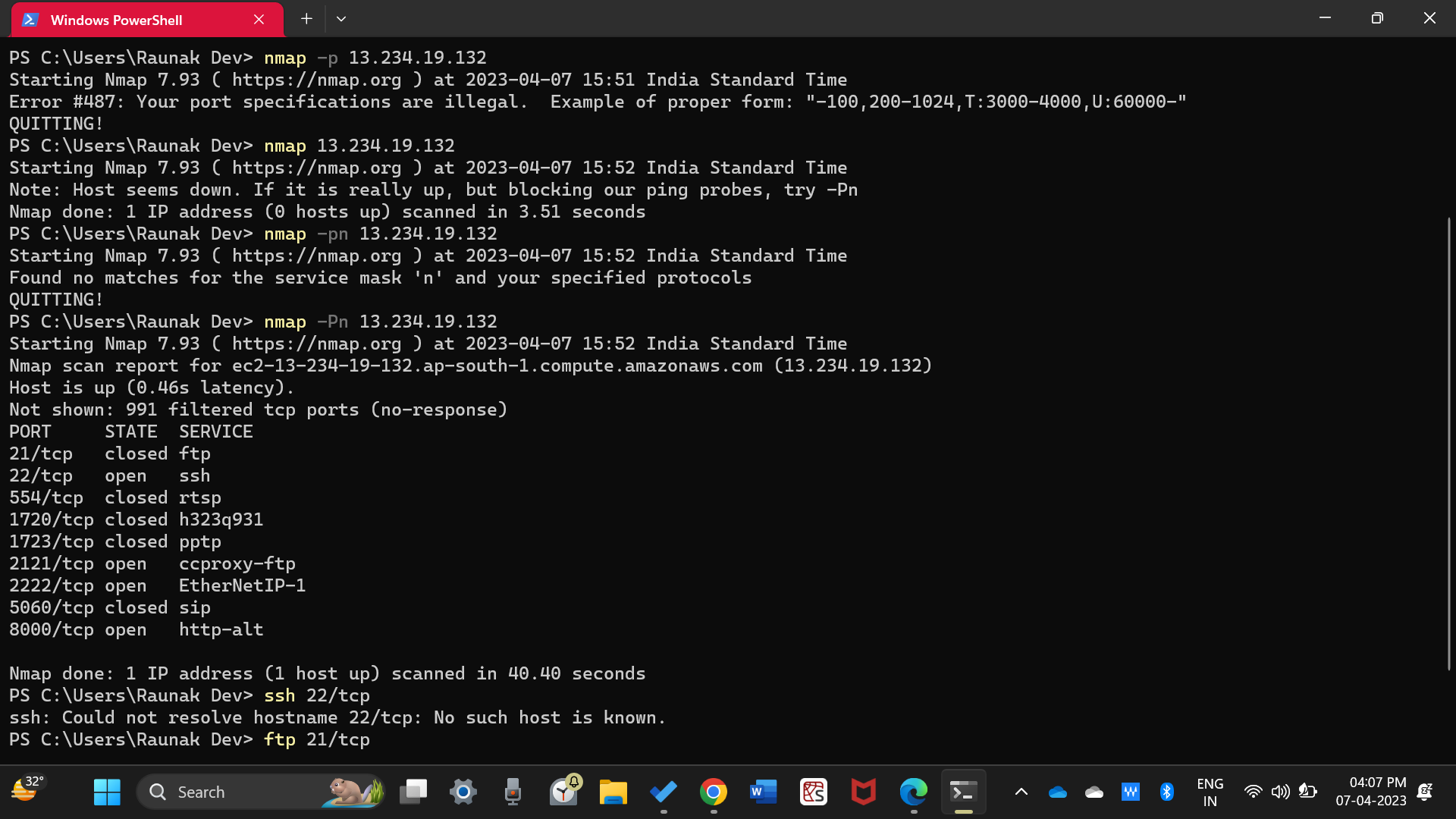
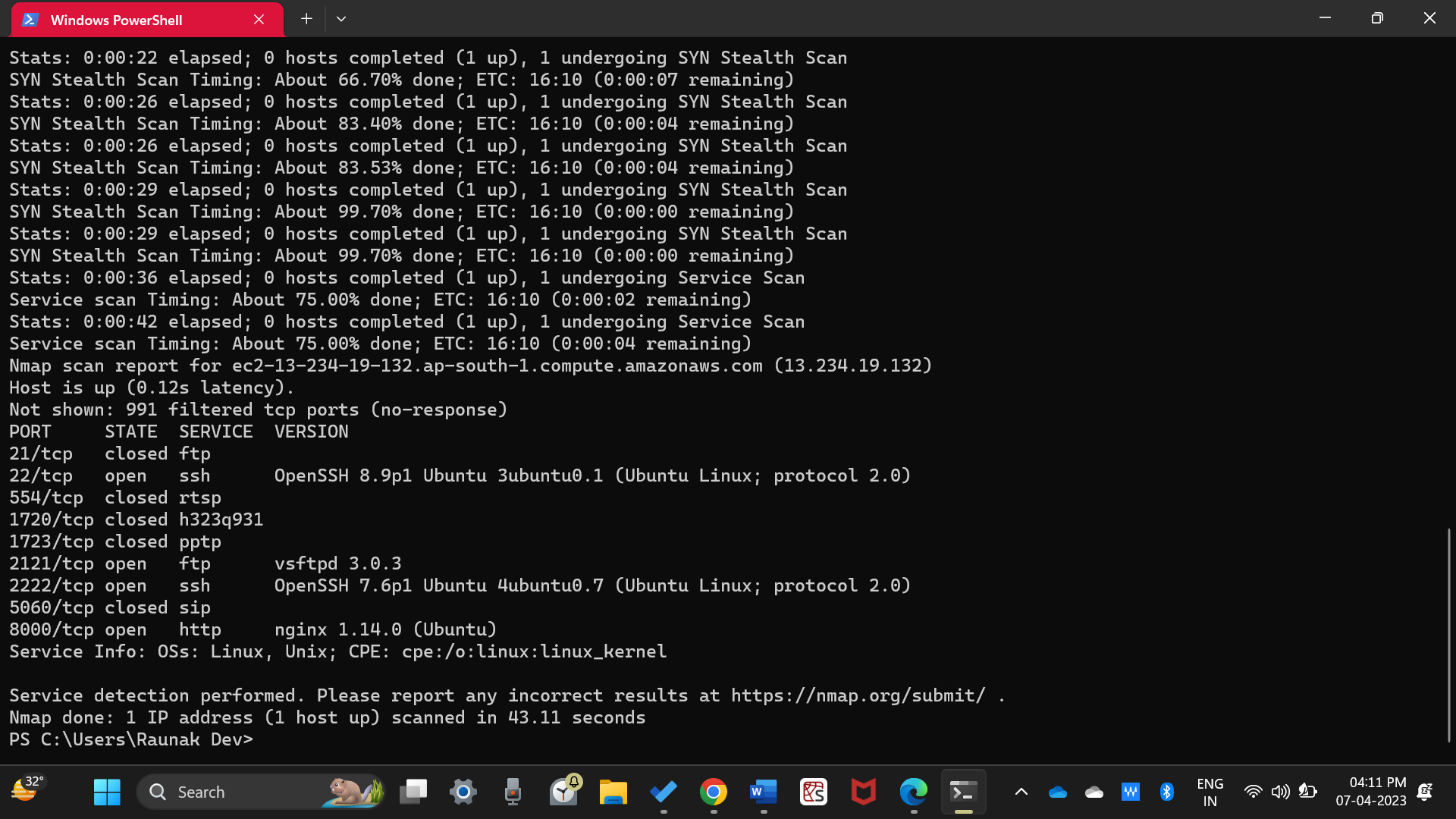
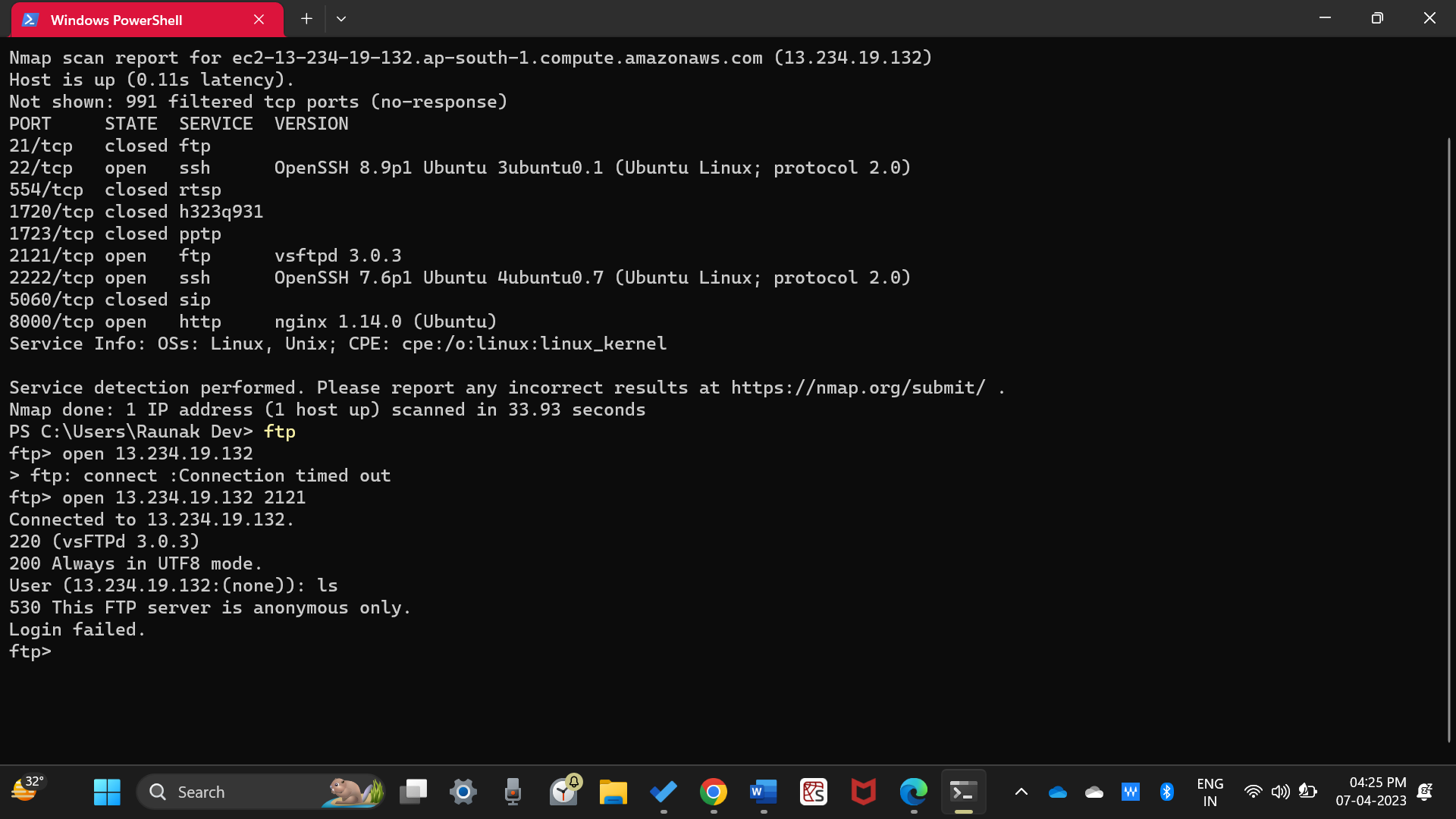
Vulnsphere challenge

First I started with an nmap scan on the given ipadress to find the list of ports that could’ve been exploited in order to find the flags. I used nmap -Pn cmmand for this to run a full scan. For the time being I used windows terminal for this but later on I used kali linux to exploit the ports.

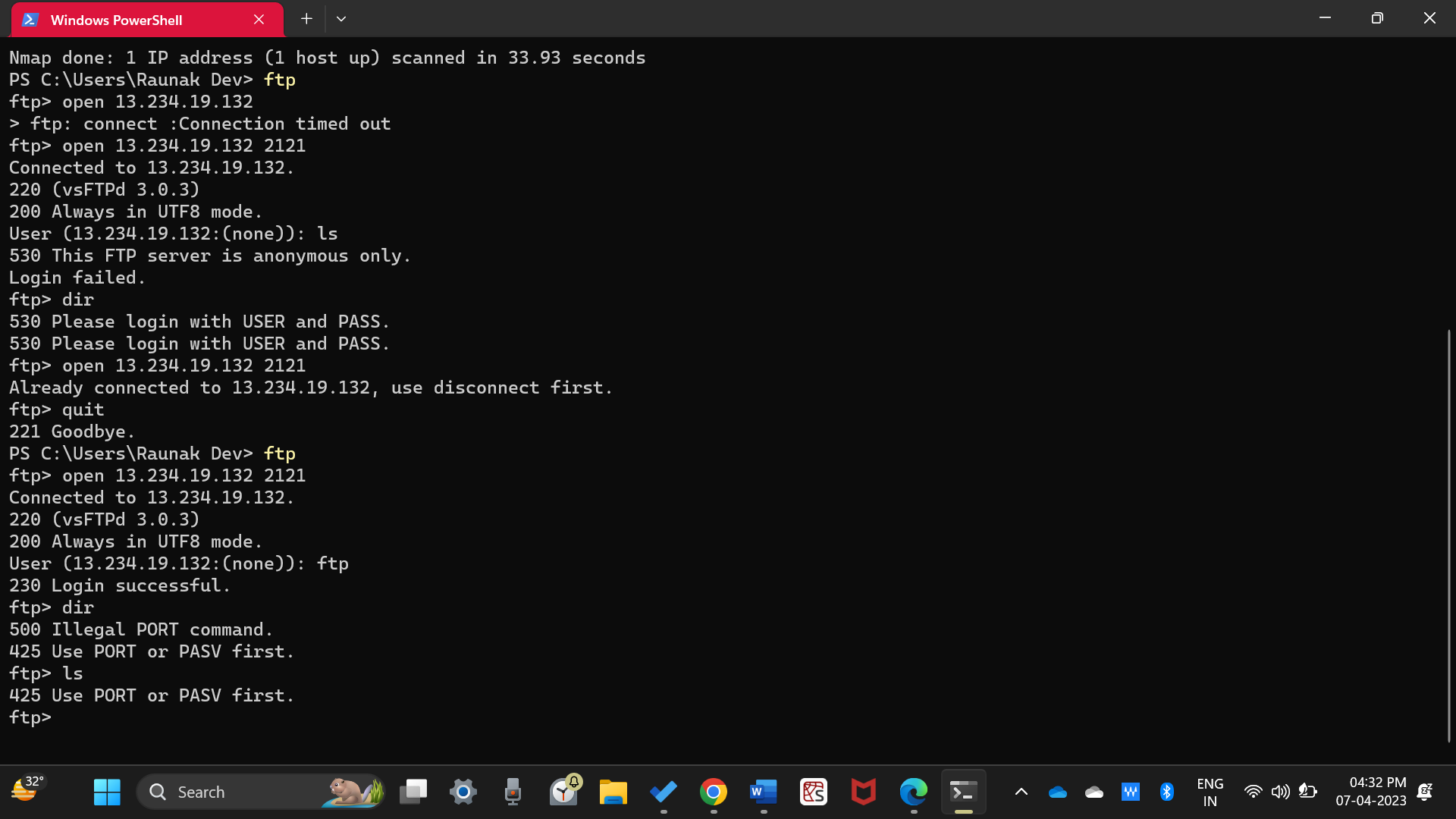


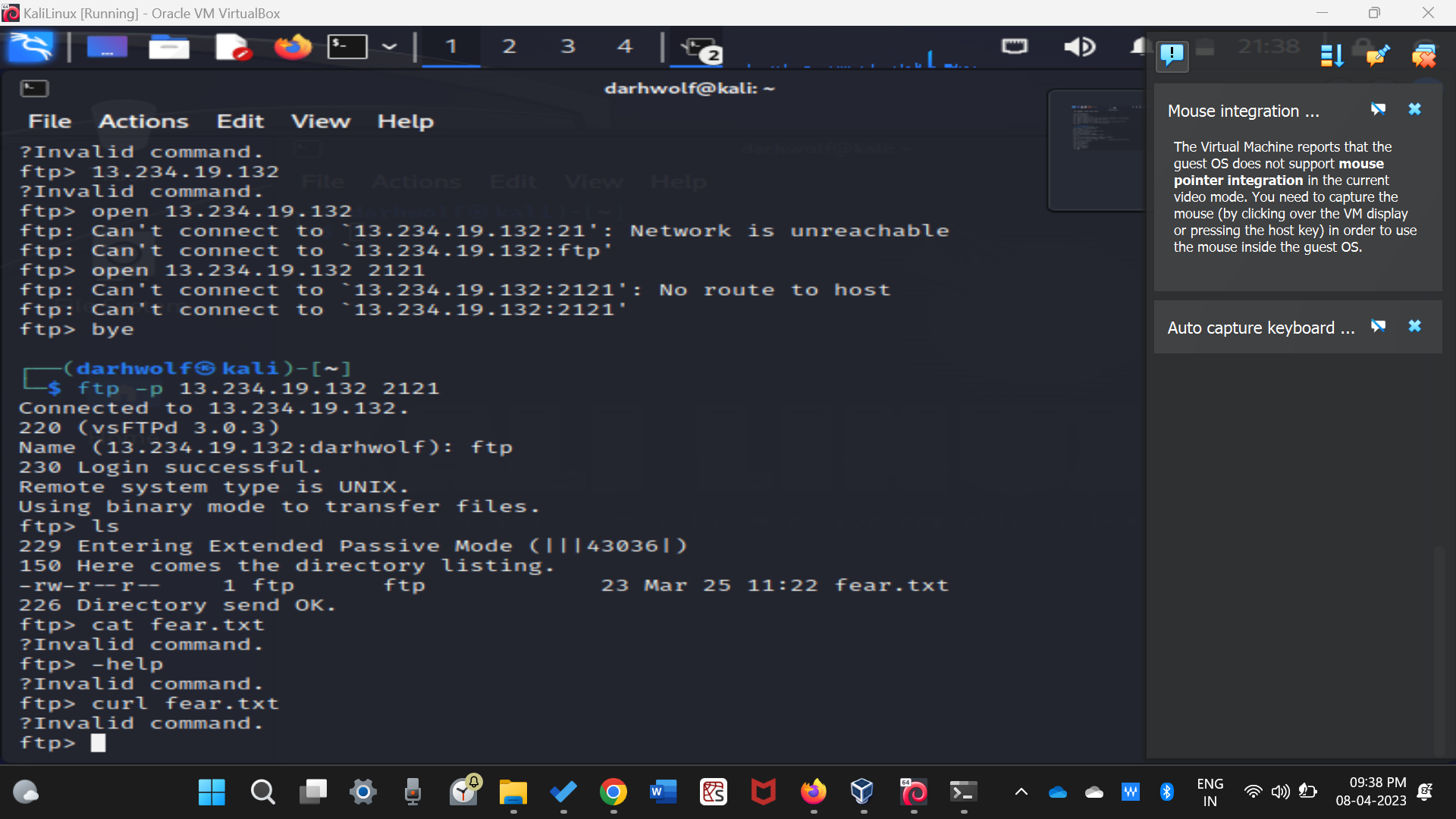


I found four open ports. I learnt that three of those ports were exploitable. I started off by connecting to port, 2121 using the ftp command. I researched on the web and I actually learnt about establishing connections to ports. I learnt about the fact that we need a username and password for connecting to the ipadress via ftp. I researched more and found out that the username is “ftp” and password is “none” in most cases. I tried that and I was finally able to establish the connection. In the windows terminal, it took me several tries. I did not give up and finally I was able to do this.



In this step, I knew that I just had to browse through the directories in this port. The flag would be in one of them. I used ls command for this to view the directories but I kept getting this error saying “USE PORT OR PASV FIRST”. I researched about this and learnt that I had to operate this in passive mode and for that I’ll need the -p command. Also, I switched to kali at this point.

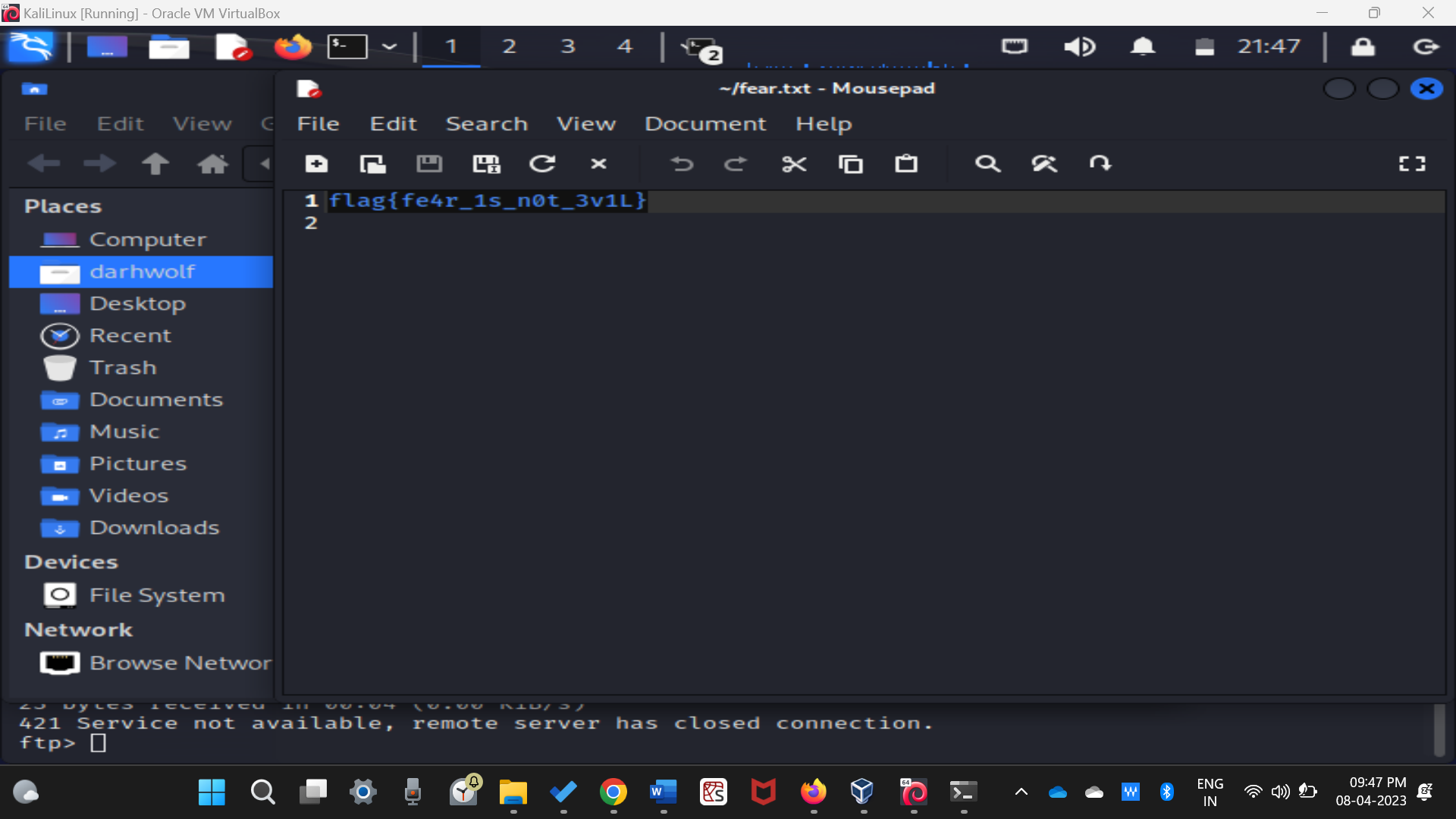


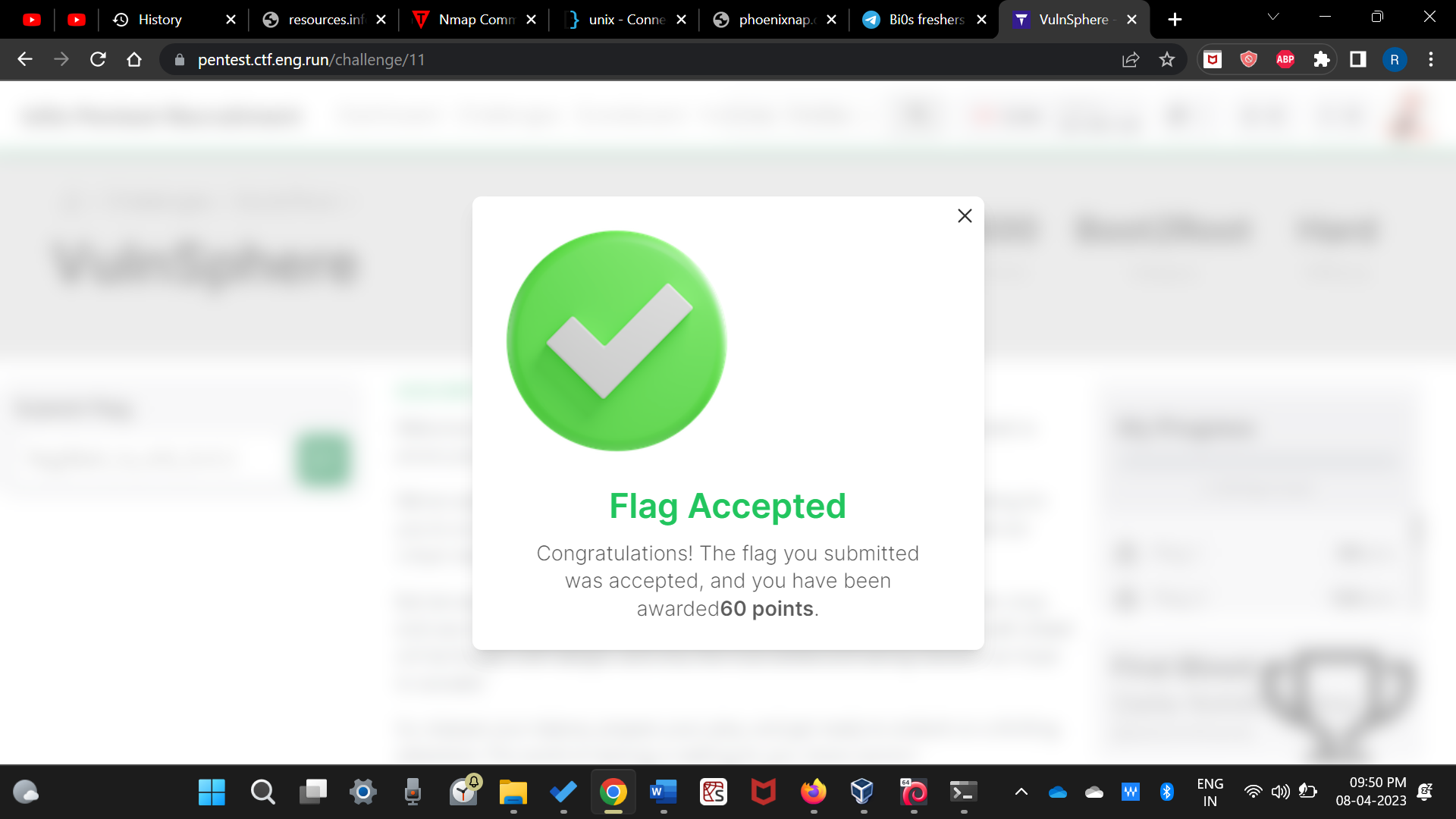


Bingo! As soon as I used the ls command, I found the text file which contained the flag. It was “fear.txt”

I just had to use the get command, “get fear.txt”. As soon as the transfer was complete, I just used the “cat” command to view the contents of the file and there it was! The first flag of my career.

<flag{fe4r\_1s\_n0t\_3v1L}>. I also viewed it in my file explorer just to be sure.





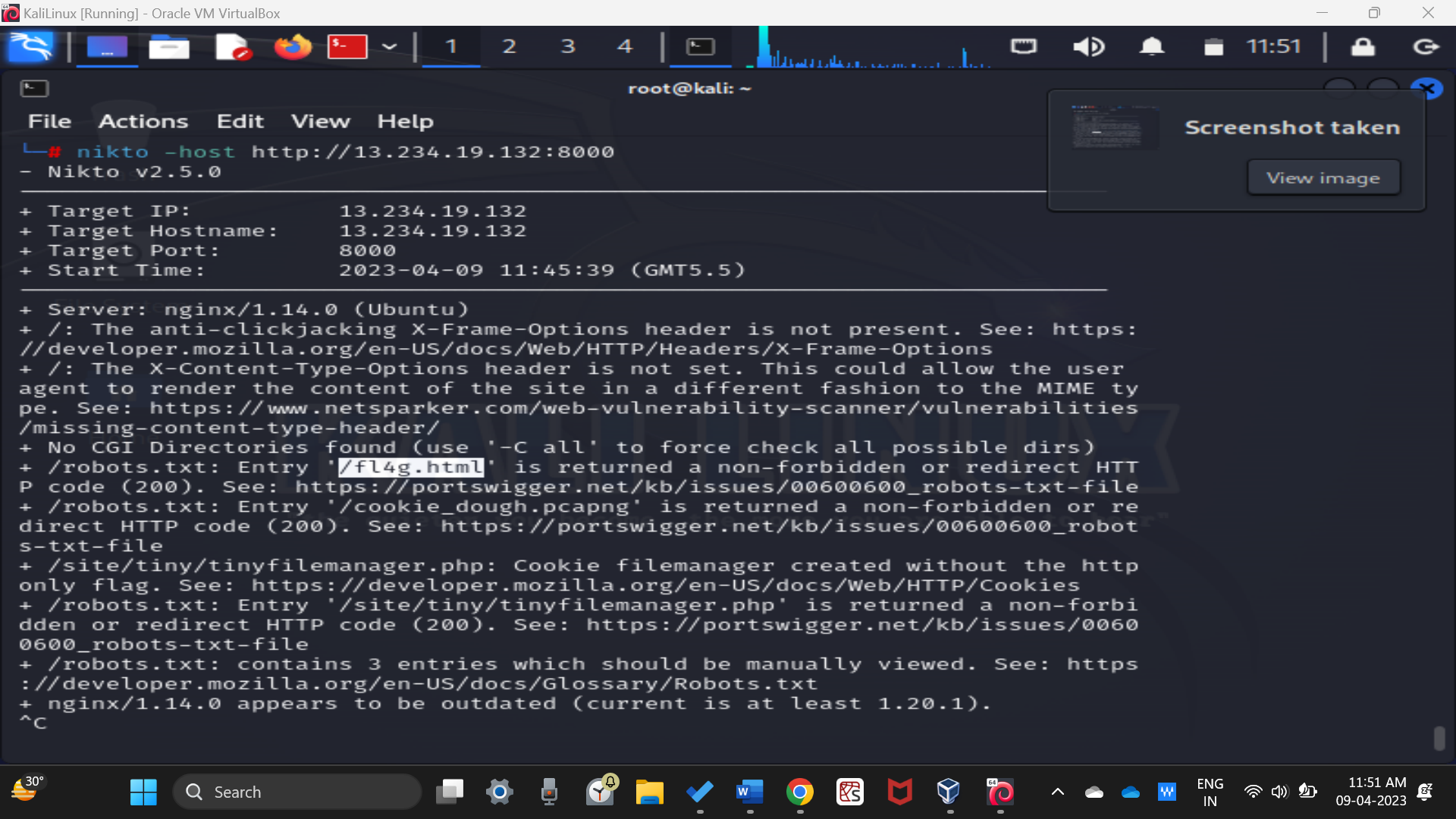
After the ftp port, I decided to exploit the http port. I researched how to do this for hours and this gave me a fair idea or I’d say an “intuition” about where this flag might’ve been hidden. My intuition was that the flag must’ve been hidden in the source codes of one the http pages linked with the ipadress.

My first attempt was to directly visit the page http/13.234.19.132 which simply did not work. It took me much time to realise that I had to mention the port number as well in order to reach the corresponding page.

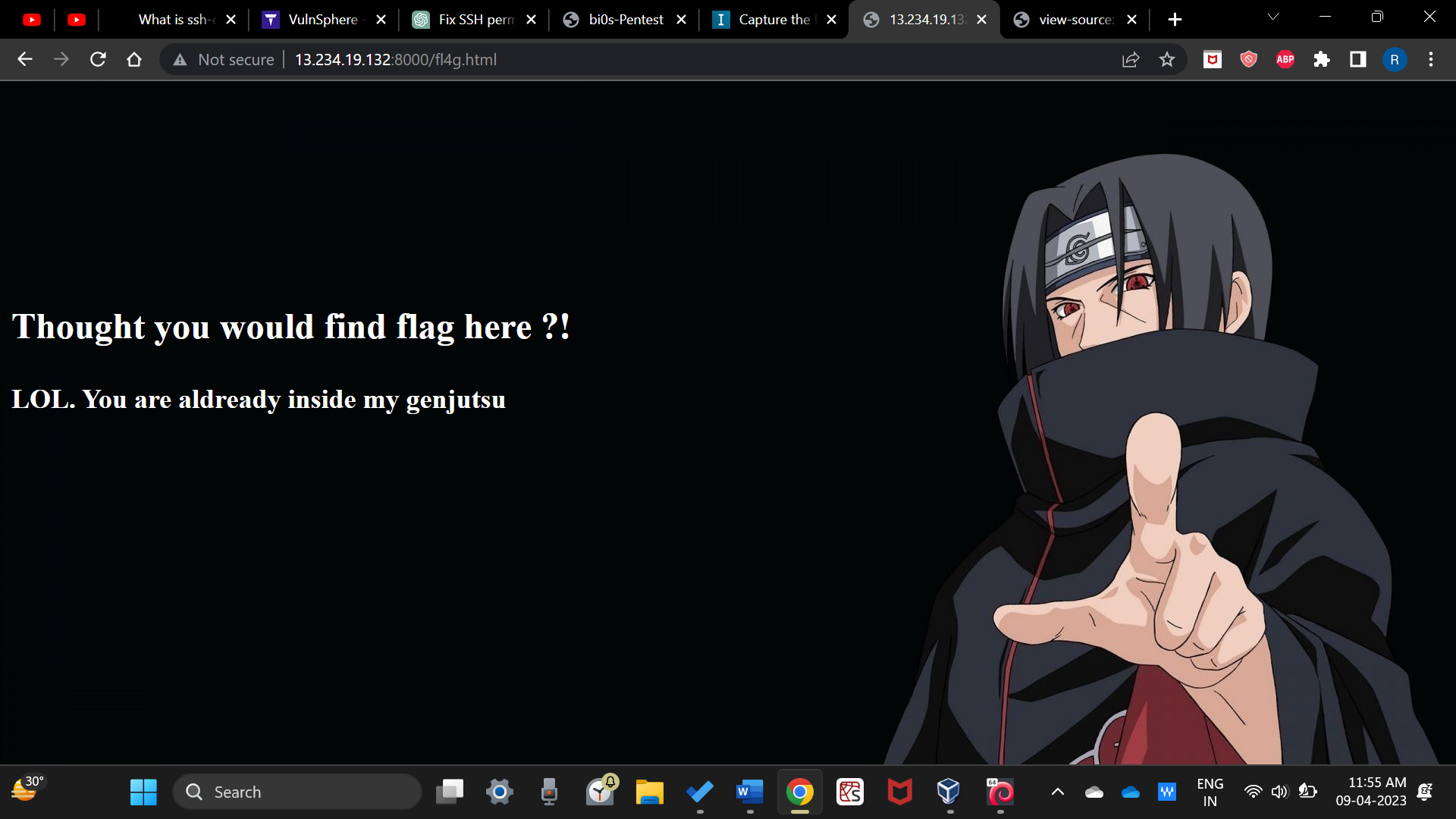
I then typed 13.234.19.132:8000. (At this point he ipadress I had this ipadress memorized in my head) And I got directed to the front page or I’d say the “hoax” page. For a moment I thought I had found the second flag. As soon as I curled the webpage, I did not find a flag anywhere. I scanned everywhere through the code but I was unable to find a flag.

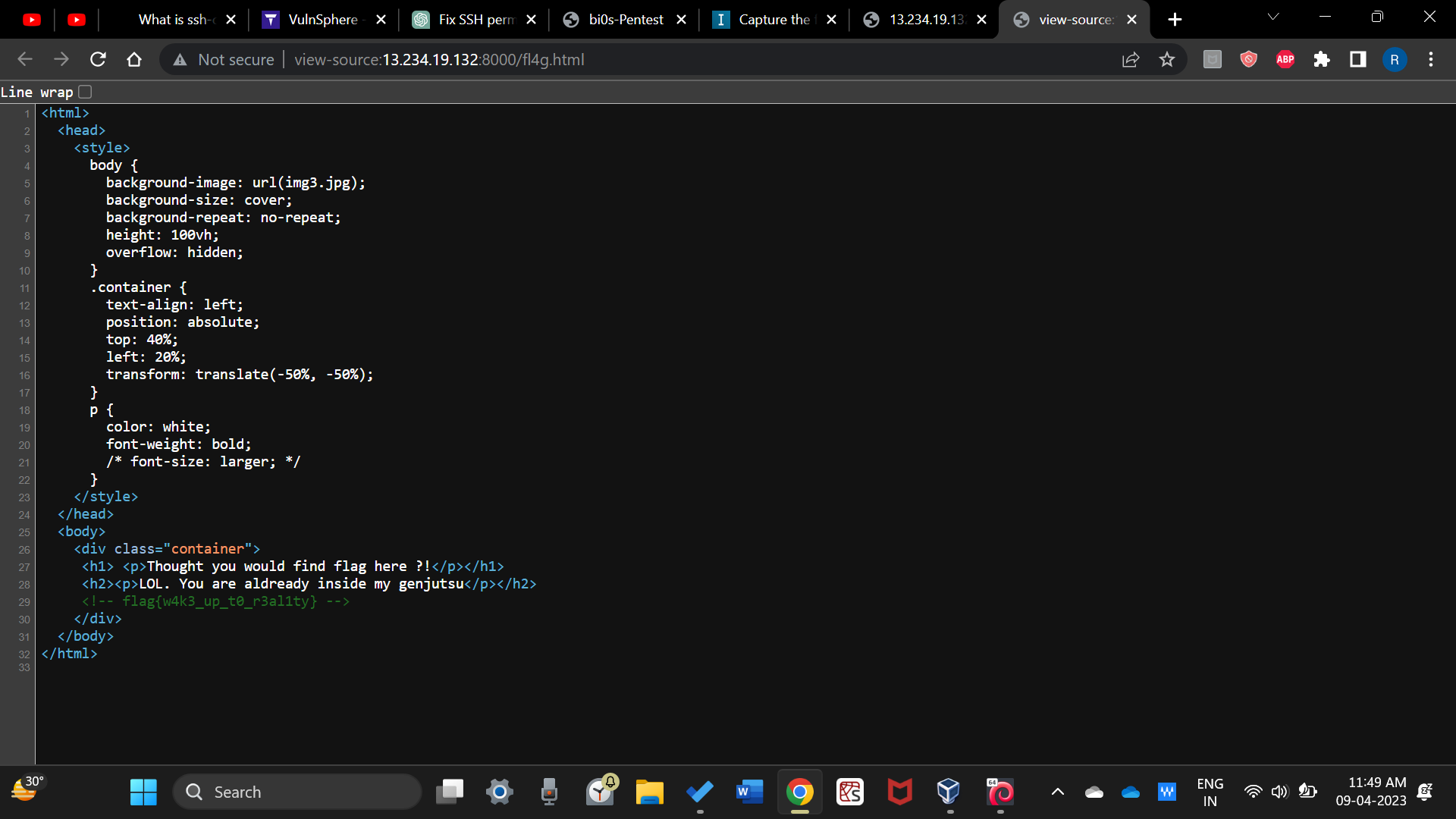
I tried again; I researched more on the web. After countless hours of browsing, I found out that there might be some extension to this webpage. Some keyword, in front of the address. For example, say, http//13.234.19.132:8000/bios.html or something. i kept getting an error saying “File not found”. At this point I knew that my next step should be to find that keyword.

After another session of countless hours of browsing, I found about the holy grail. The nikto scan! I learnt about it and put it into action using the command, “nikto -host 13.234.19.132:8000”. And there it was! In the midst of the text was the keyword I was looking for. “/fl4g.html”.

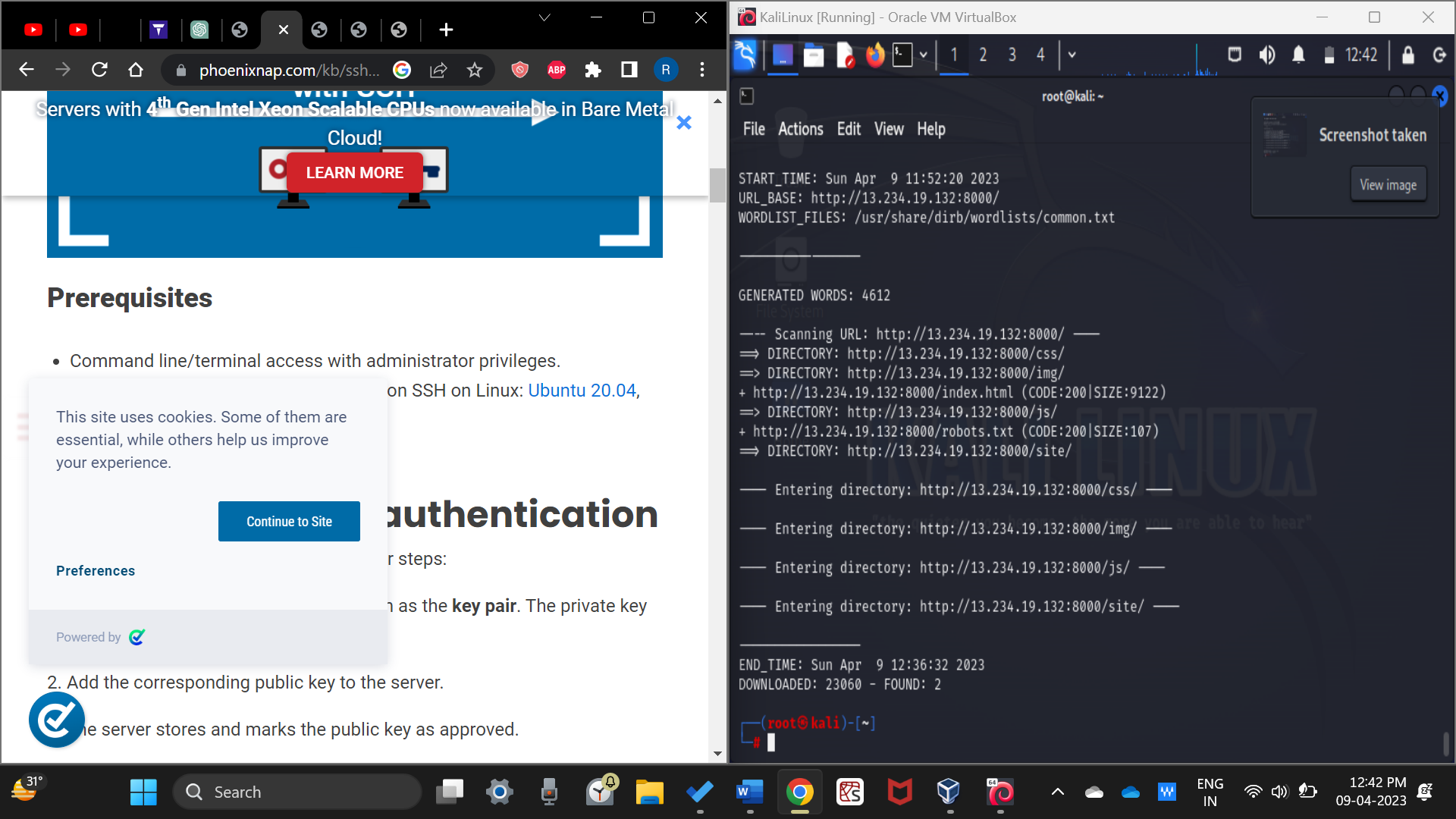


I quickly opened my browser and typed the adress there. As soon as the webpage opepened and I read, “Thought you’d find a flag here”, for a moment I thought this was another hoax page. But this time instead of curling in the terminal, I decided to dirctly view the source code in the browser itself because the text is coloured which makes it easier to find the flag. There it was, the second flag in green coloured text. <flag{w4k3\_up\_t0\_r3al1ty}>



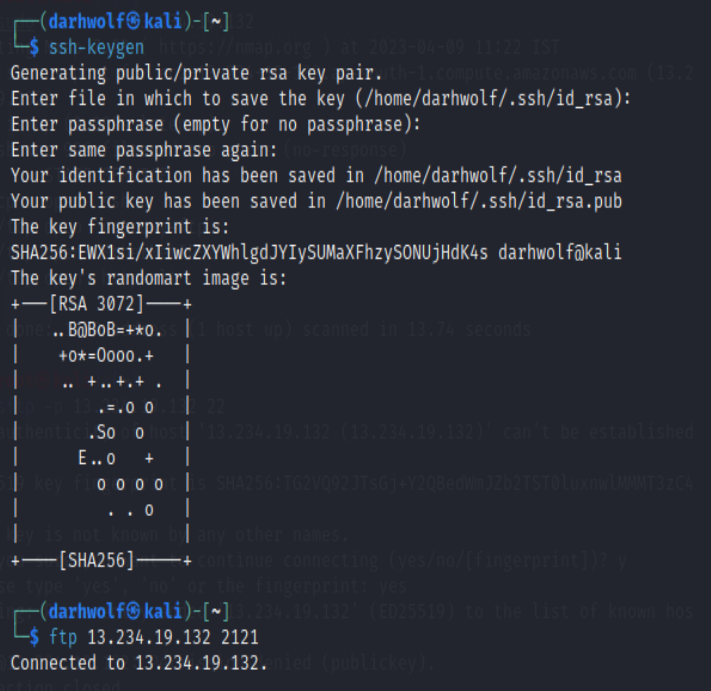


While learning about the nikto scan, I also learnt about dirb scan. But there wasn’t much I could find with this. The scan went on for a while and there were just some directories that it downloaded.

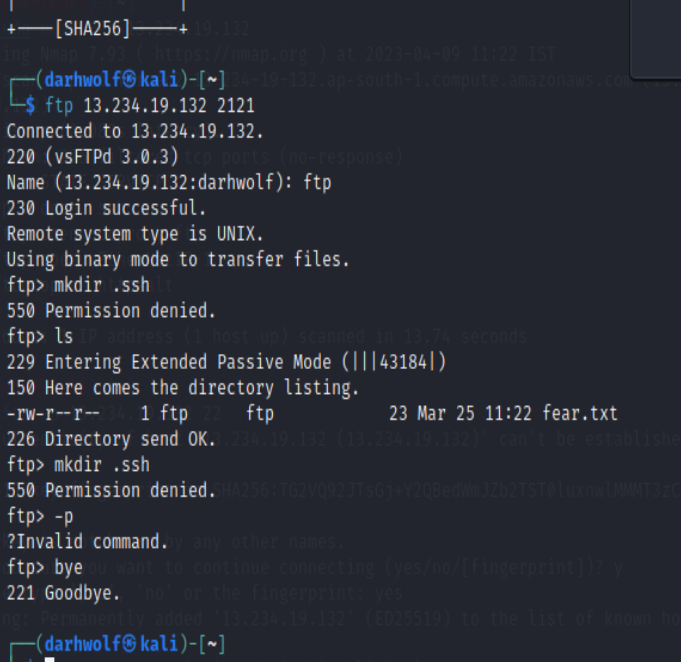


Now it was time to exploit the ssh ports. I tried to connect to the port directly using ssh command but I was unable to gain access. I kept getting an error saying “publickey”. “accesss denied”.

I researched about this and I learnt that first I need to generate the publickeys on my device and I have to upload publickeys on the target device. I generated my keys using ssh -keygen command. After that I tried to upload those to the host device using ftp. I’m thinking I might be wrong here but I still Gave it a go.



I used the mkdir command but I faced an error saying “Permission denied”.



There’s still quite a few thing that I might have to learn about connecting via the ssh ports.

This was my approach for now.

See you at the top!

-Raunak Dev