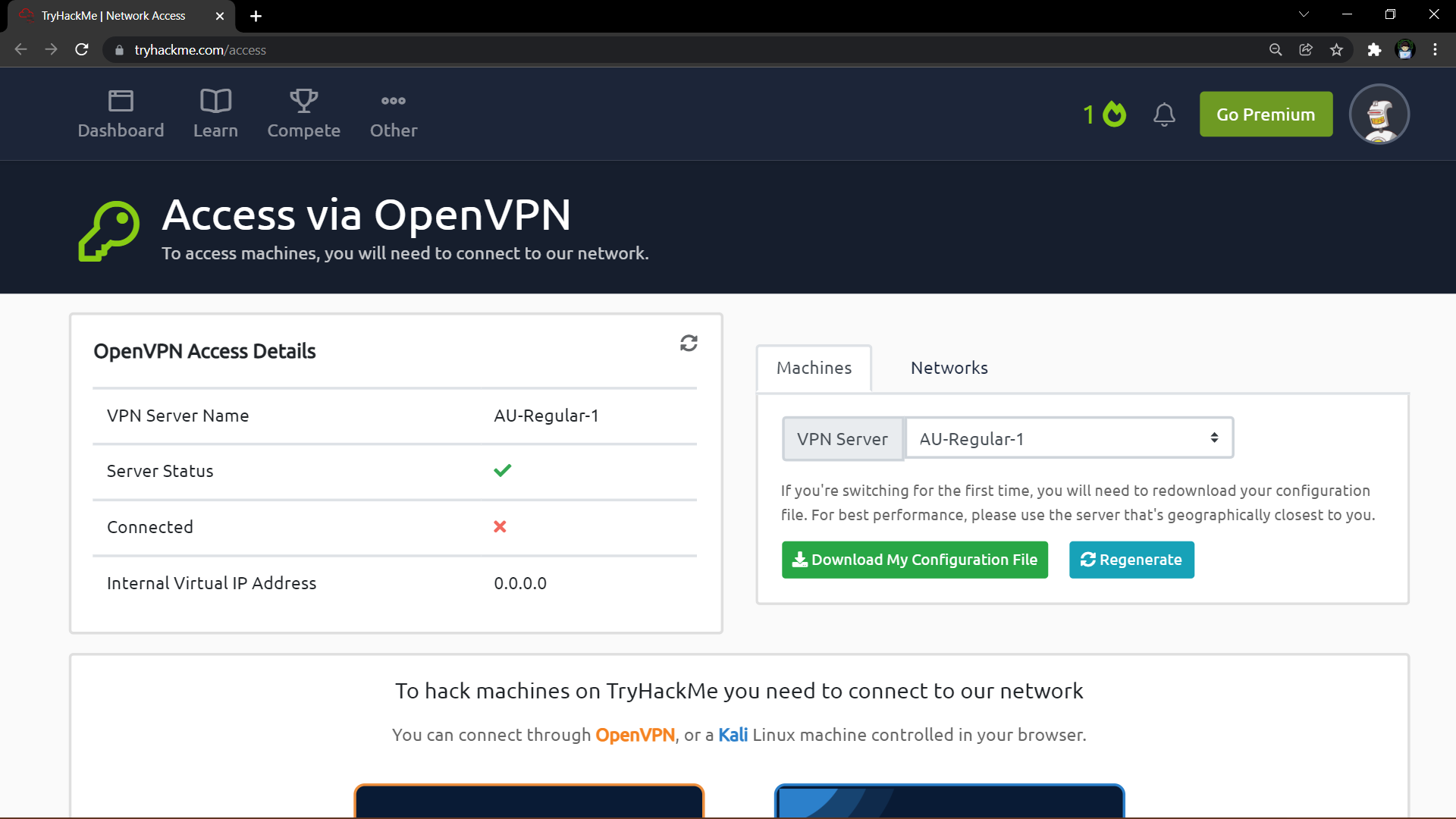
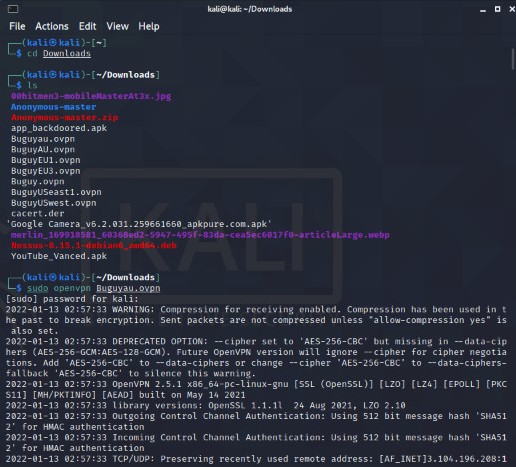
**Penetration of Headless**

**Step 1 :** Connect to open vpn using configuration file

* Download configuration file."https://tryhackme.com/access”



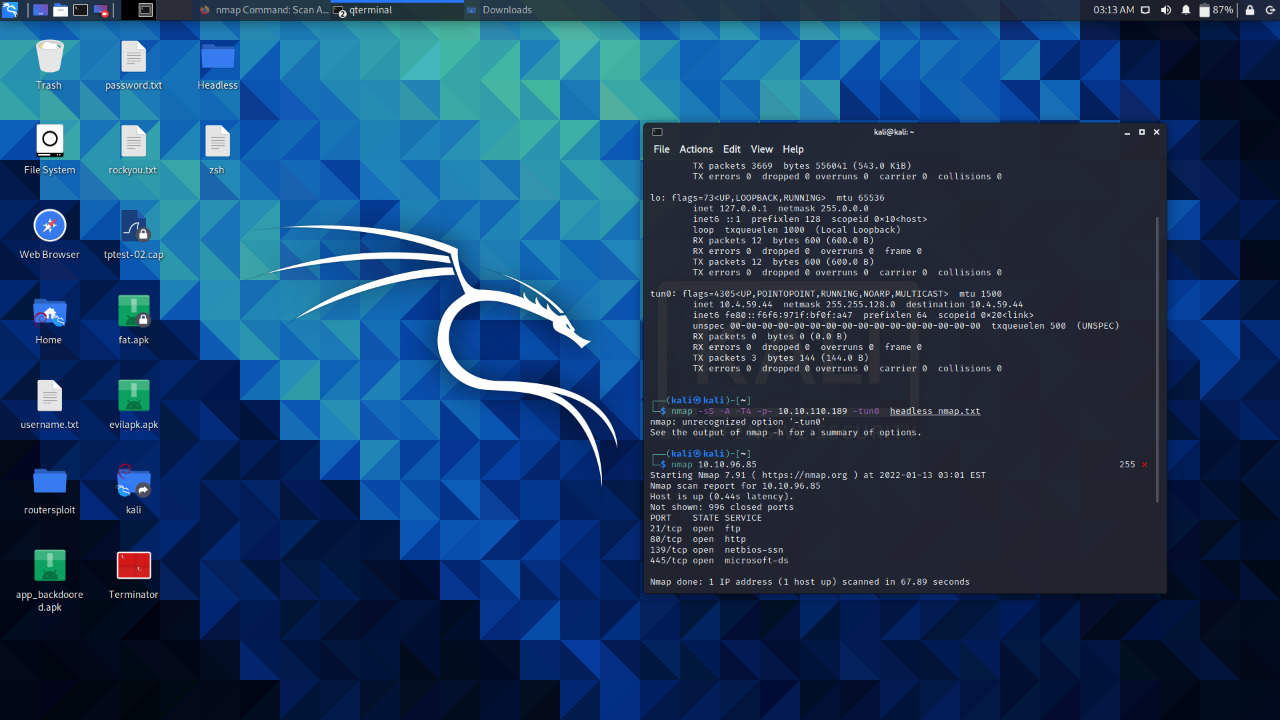
* Fire up Kali Terminal.
* Move to the directory in which {filename}.ovpn is Downloaded.
* Use cmd ~ sudo openvpn Filename.ovpn



* The Openvpn is connected successfully.

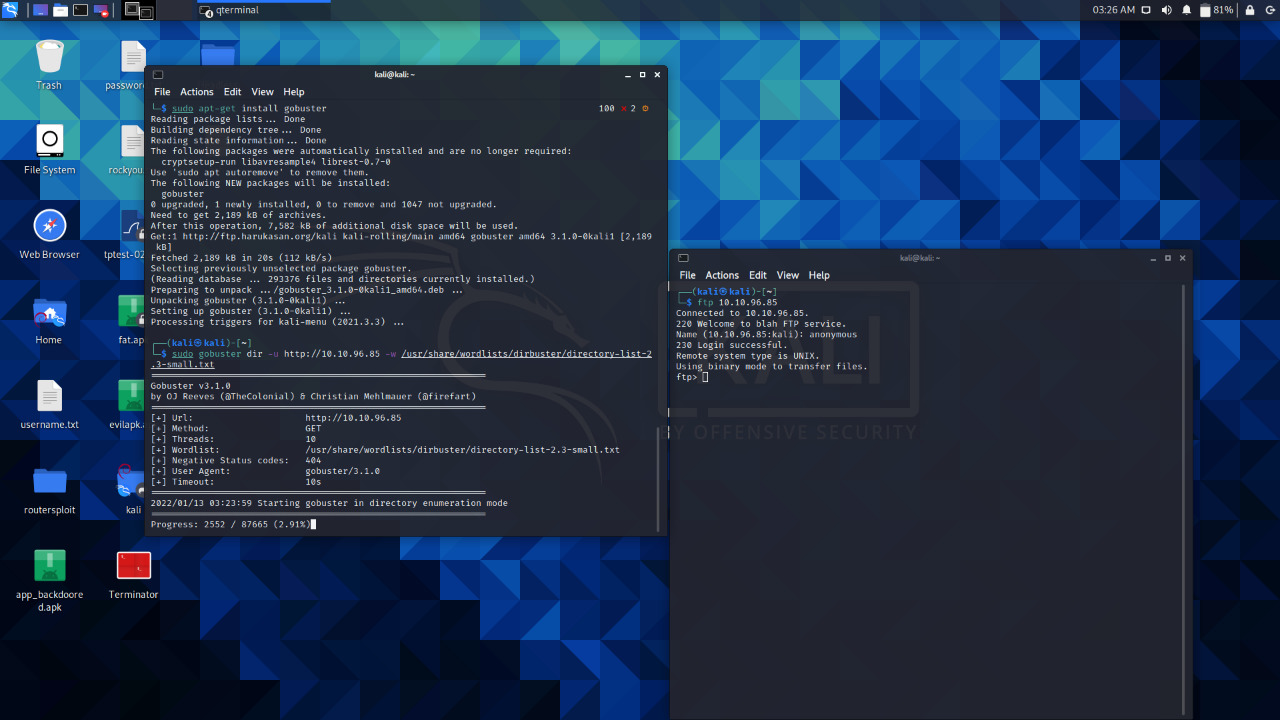
**Step 2 :** Start enumerating machines by simple nmap scan considering all Ports.

* Use cmd ~ nmap{ip address}



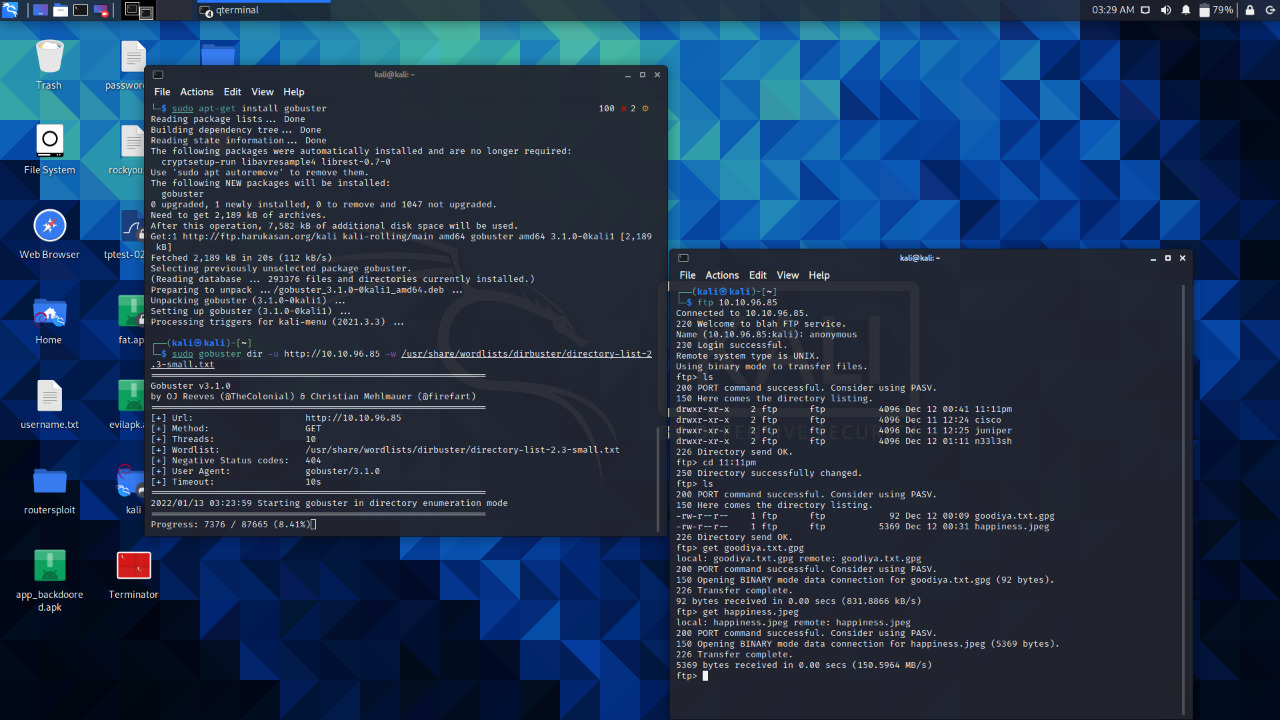
**Step 3 :** Since we can see from the nmap scan that the Ftp server allows anonymous login we can try to search for some files.

* Use cmd ~ ftp{ipaddress}



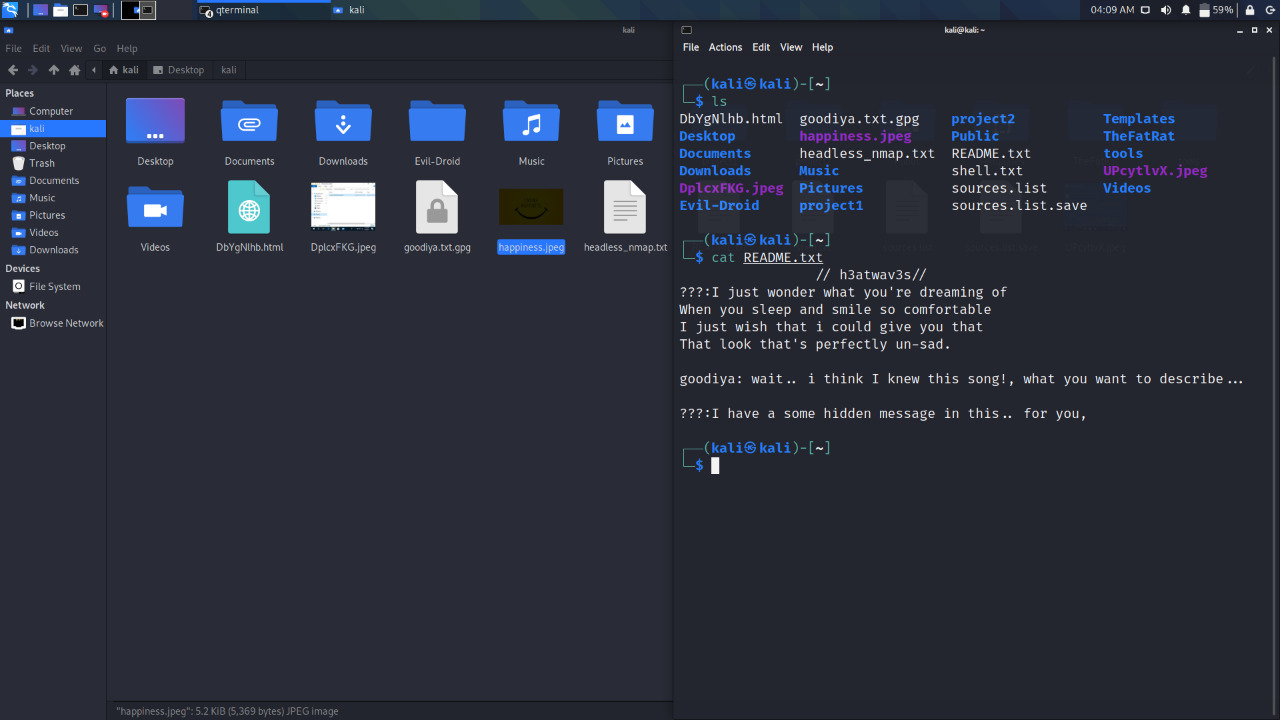
**Step 4 :** Remote login successful

* Use cmd ~ ls to print current working directory
* Use cmd ~ ls -la to print hidden directory
* Use cmd ~ get{filename.extension} to download files
* Use cmd ~ bye to end session

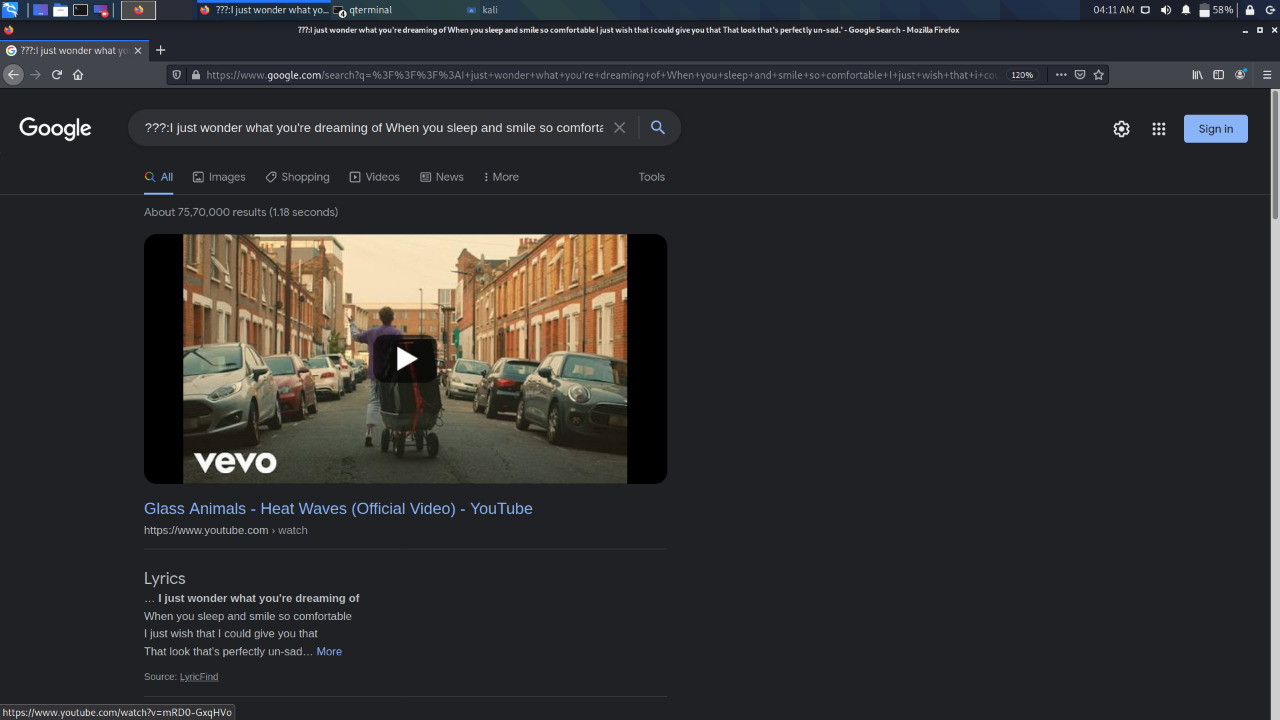
****

**Step 5 :** Exploring the hidden files.

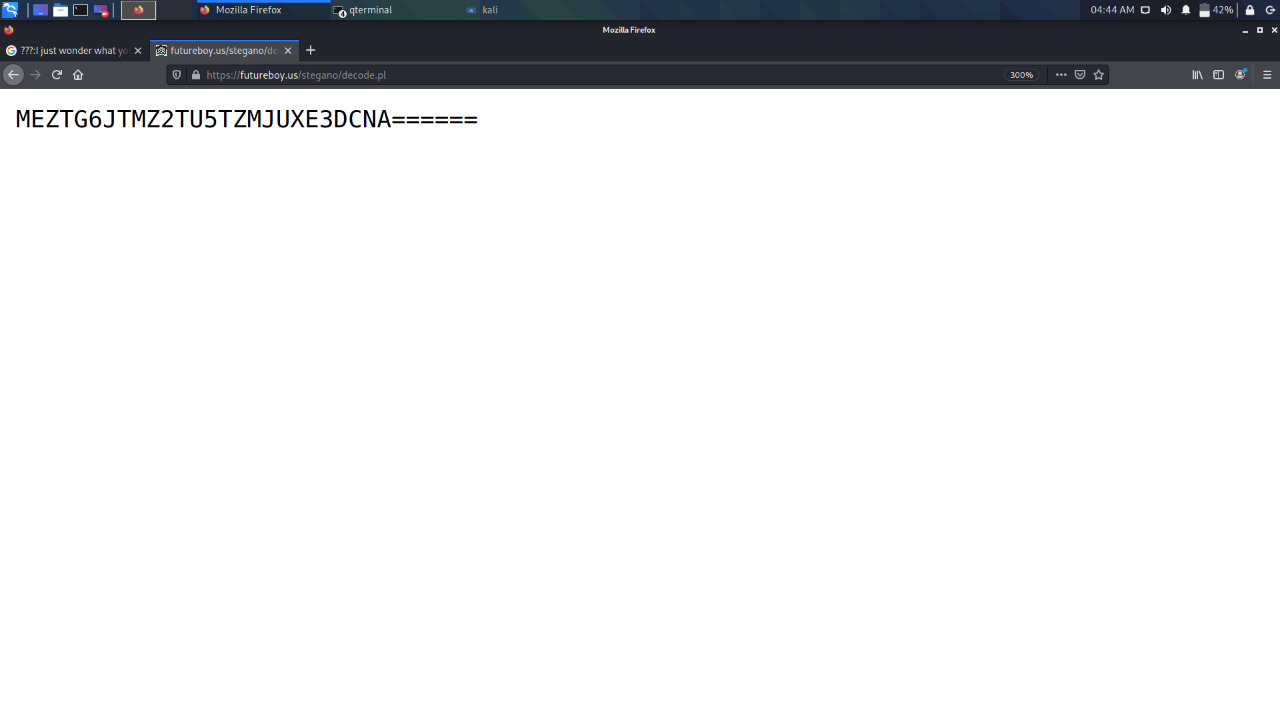
* Readme.txt



* Searched for the text on Google



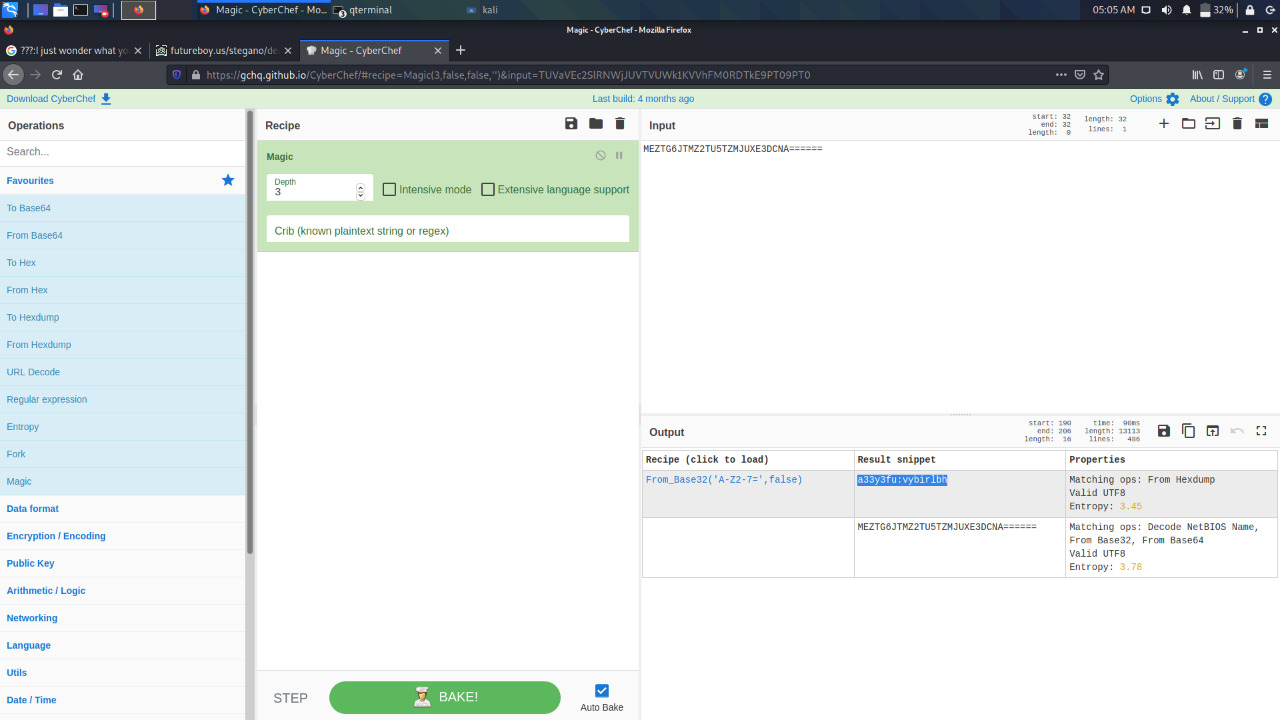
* Uploaded Happiness.jpeg steganography tool-<https://futureboy.us/stegano/decinput.html>
* Passphrase tried glass animals / heatwaves/ h3at wav3s = h3at wav3s



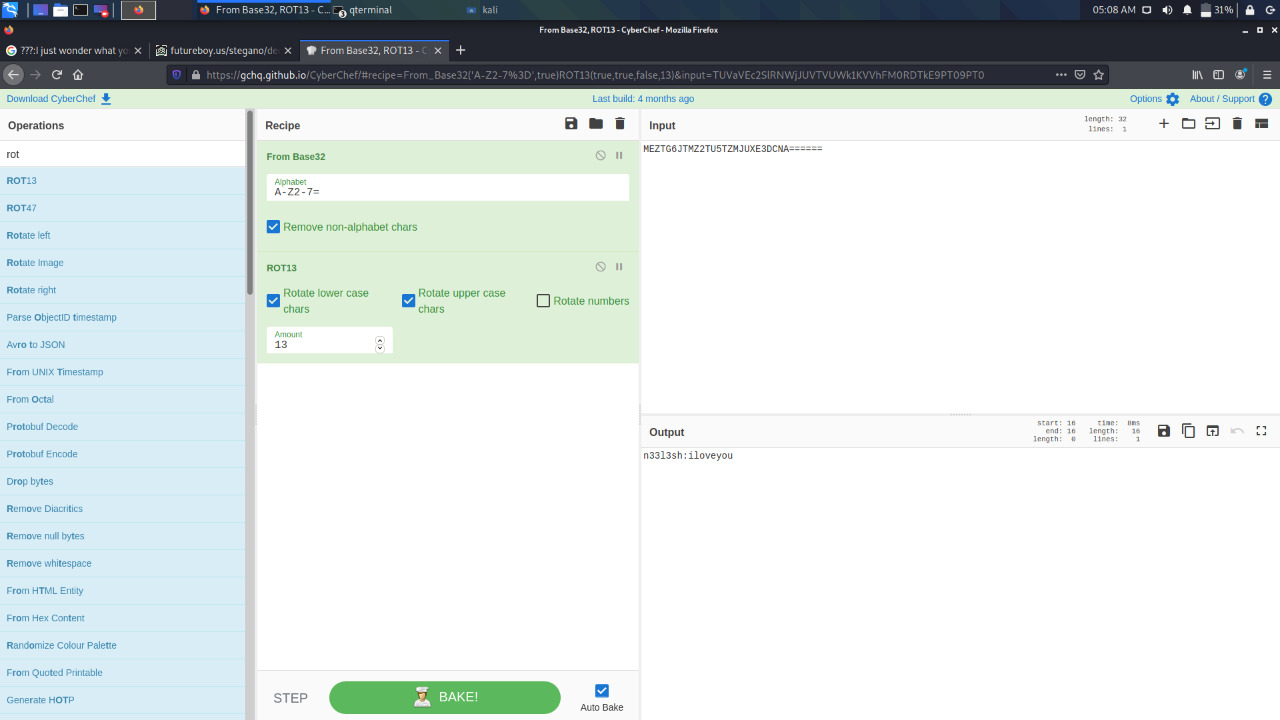
* Got the String

**Step 6 :** check it on cyberchef

* A function called "Magic" - "The Magic operation attempts to detect various properties of the input data and suggests which operations could help to make more sense of it.

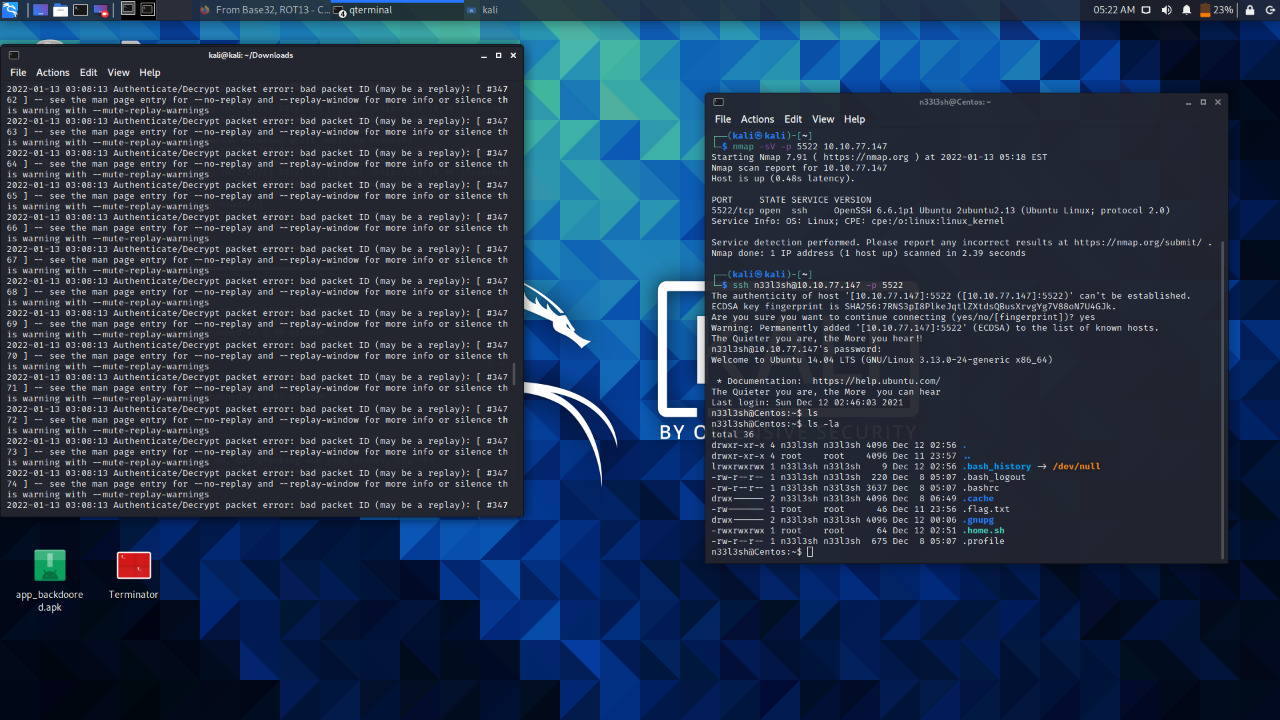


* The Base32 string looked like a rot algorithm(Rotation cipher) because I had come across a directory called : "n33l3sh" - "a33y3fu"
* Rot13 Decoding - n33l3sh:{PASSWORD} .

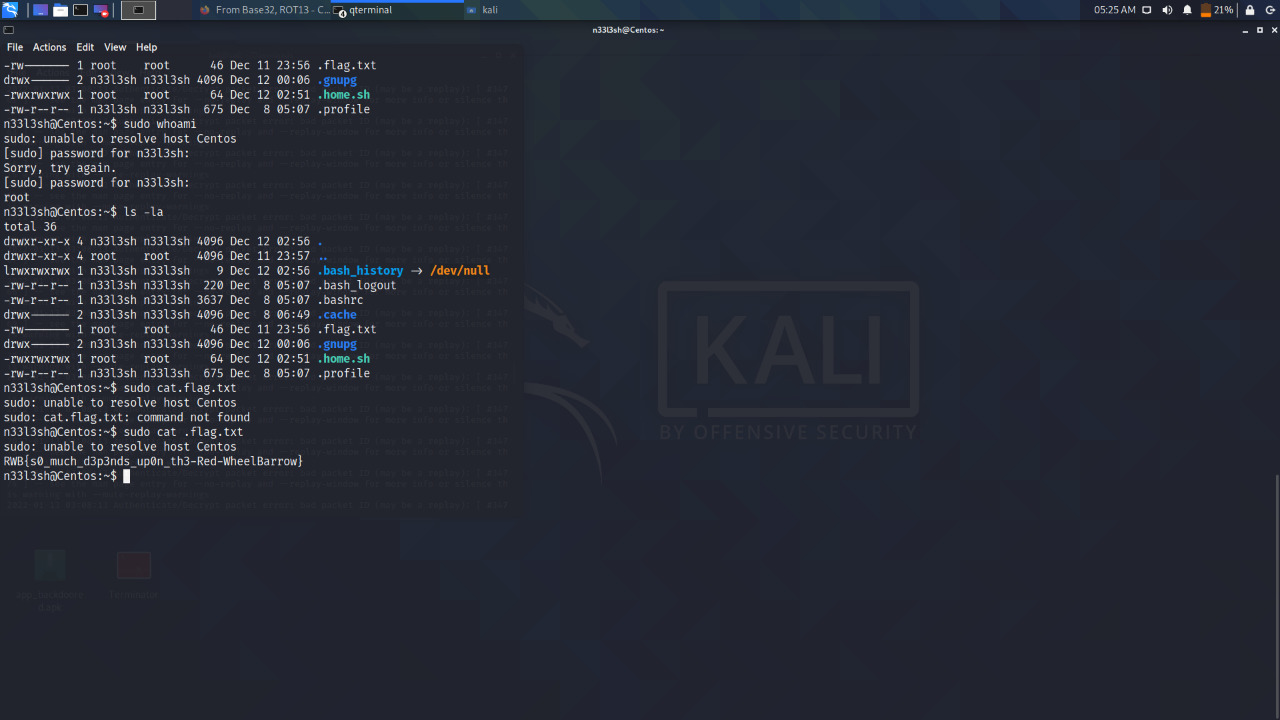


**Step 7 :** Trying to Login in via SSH using the port 5522.

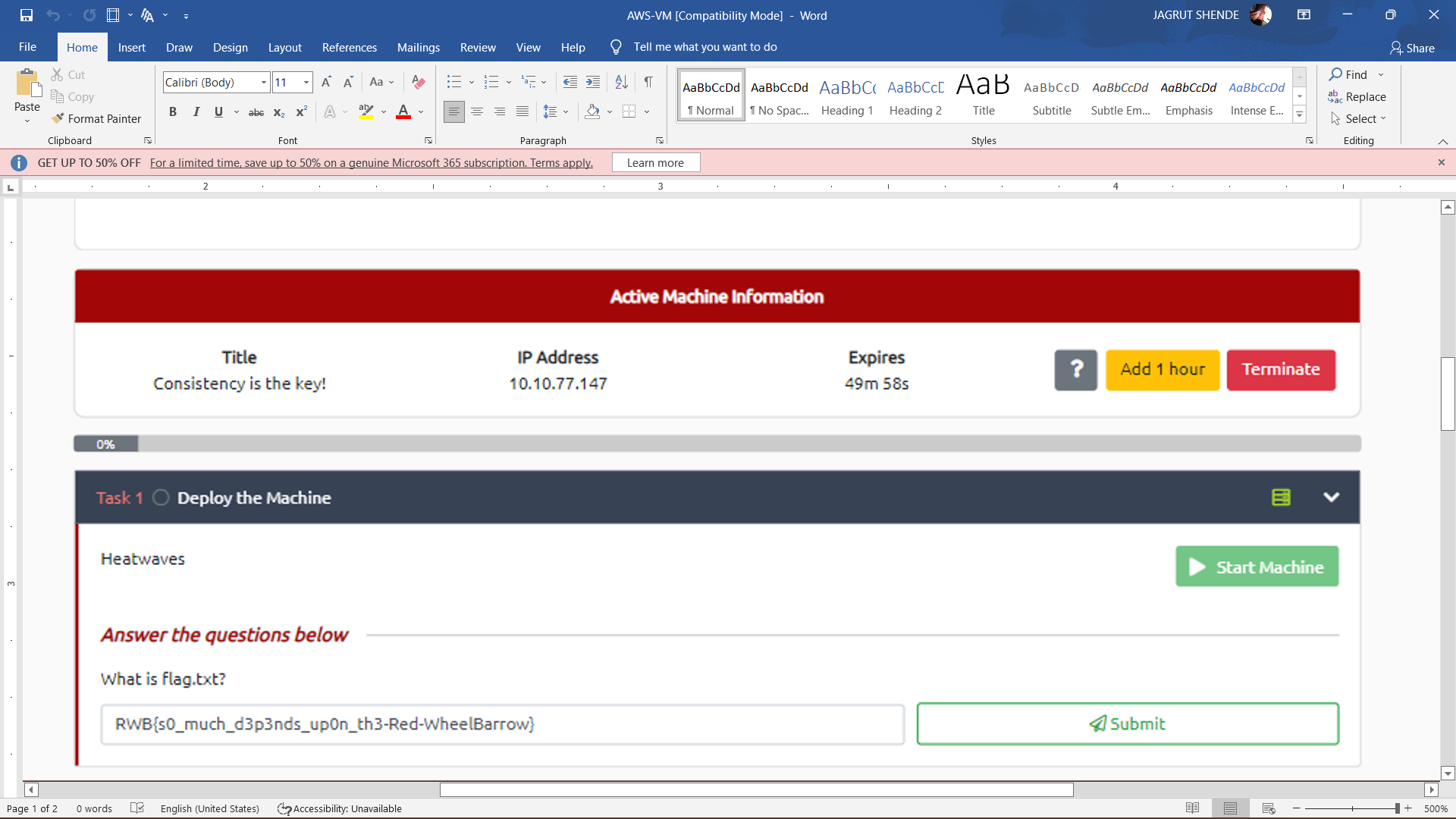
* ssh n33l3sh@{ipaddress} -p 5522



* Finally got the Flag file - '.flag.txt'
* After trying to cat.flag.txt



* Got the flag.



* Submit the flag.

