Here is the step on how to setup the “Autonomous-Penetration-Testing-using-Reinforencement-Leaning” Codes

1. Approach github link <https://github.com/yeeticusyey/Autonomous-Penetration-Testing-using-Reinforcement-Learning> to download all the branch

Graphical user interface, text, application, email

Description automatically generated

1. Or using the command ‘git clone https://github.com/yeeticusyey/Autonomous-Penetration-Testing-using-Reinforcement-Learning --recursive’ on the kali terminal. Graphical user interface, text

   Description automatically generated
2. Cyber Battle Sim should be important auto as a Submodule. But if it didn’t, run” git submodule update –init’
3. The code could be run using any python editor, but Jupyter Notebook will be recommended. Install it using command ‘sudo apt-get install jupyter-notebook’
4. Install Gym module to Kali using ‘sudo pip3 install gym’Text

   Description automatically generated with medium confidence
5. Open jupyter notebookGraphical user interface, text

   Description automatically generated
6. Open the folder /Autonomous-Penetration-Testing-using-Reinforcement-Learning/Modifications/DemoGraphical user interface, text, application, email

   Description automatically generated
7. My\_ctf.py is for the automation of the nodes. While runme.ipynb and runme2.ipynb are two files to generate the cyber battle Simulaiton. With runme2.ipynb as an advance version with Deep learning and Deep Q learning.

my\_ctf.py

edit the parameter of addnode to filename of future nmapscan report and nessus report.

Graphical user interface, text, application, email

Description automatically generated

1. Open Runme or Runme2.ipynb and run it cell by cell. Take note of this line wait till Download complete before procceeding to the next one. Graphical user interface, text, application

   Description automatically generated
2. Run alll other cell and output will be displayedGraphical user interface, text, application, email

   Description automatically generated