

Firewall Implementation in python

- When you initially execute the program file "firewall.py", the predefined set of websites will be blocked.

Dependencies

- os
- re
- subprocess
- SQLAlchemy

Execution steps

- You can execute the program containing the firewall implementation using the following command after installing the dependencies,

```
sudo python3 firewall.py
```

- After executing the program, the predefined streaming sites get's blocked and you will see the following set of options from which you can select and execute the command which you would like to,

[+] Enter any of the folowing commands :

- > 1 <url of website> : To block a new website for the host machine.
- > 2 <ip address> : To block a new ip address for the host machine.
- > 3 <url of website> : To unblock a website for the host machine.
- > 4 <ip address> : To unblock an ip address for the host machine.
- > 5 : To block alternate sites of the previously blocked websites by brute force approach.
- > 6 <string> : To block alternate sites of the previously blocked websites by string matching approach.
- > 7 : To view the iptable rules for the blocked websites.
- > EXIT : To close the firewall and restore the iptable rules.

- You can enter the command by first providing the option number which you want to execute followed by the required argument. For example,

```
command : 1 iitj.ac.in
```

- The above command will block the network traffic from the host "iitj.ac.in" using the *iptables* functionality

Detecting SQL injection using machine learning

- You can execute the "SQL_Injection.ipynb" file containing the implementation of detecting the SQL injection using machine learning models in google colab, jupyter notebook etc.
- The dataset used to train the models can be found [here](#).
- To import the dataset, you can just add the above provided folder to your google drive or to your working directory and change the path where the data is imported in the ipynb file.

Machine learning models

- Logistic regression
- Random forest
- Support vector machines (SVM)
- Naive Bayes
- Convolutional Neural Network (CNN)

After importing the dataset, you can execute the code which trains different machine learning models defined above on the data and reports the accuracy scores and F1 scores for different models. And the models were compared based on their performance scores and model with best performance in terms of accuracy score and F1 score is selected.