**NETWORK TRAFFIC ANALYSER FOR DETECTING DOS ATTACK USING MACHINE LEARNING**

**ABSTRACT: -** At any given time the traffic entering the network may be genuine or can be some malicious traffic. There may be times when a definite pattern is established when the malicious traffic is highly active (based on timelines). It becomes necessary to analyze all the incoming traffic into a particular network/server to identify the types of traffic entering so that proactive measures can be taken to safeguard our systems against harmful traffic. NETWORK TRAFFIC ANALYSER analysis the incoming packets whether it is normal traffic or some malicious packets in particular denial of service attack. Using machine learning the system is trained to detect DOS attack. The tools used to achieve this are Tshark, Pandas, Matplotlib and Scikit learn. Using Tshark the incoming packets are captured and sent as a CSV file to Pandas which perform data analysis to differentiate normal packets and DOS packets and then we feed the system with DOS packets by using Scikit Learn. Later, we visualize DOS packets using Matplotlib.

KEYWORDS:-NETWORK TRAFFIC ANALYSER, NETWORK TRAFFIC DETECTION-, MACHINE LEARNING