Abstract

In the modern era of computer networks, the prime concern has always been on providing a secure communication between the server and the client computers, ensuring the necessity that the resources available to those who require it is never compromised. But, it has been observed that a network may be targeted by malicious users who may consume a large amount of bandwidth so that the legitimate users are deprived from using it, when required. Thus, it is necessary to deploy a good Intrusion Detection and Prevention System (IDPS) to monitor the traffic flow to detect any such harmful activities by outside and inside users of a particular network. We have seen that tools like Snort can be very helpful in analysing the network traffic to inspect the receiving and outgoing packets in order to determine the behaviour of various sources using the services of a network. Here, we have introduced a method to verify if the bandwidth consumption in a network by any user is critical to the overall consumption of it. We have validated our approach using a simulated environment created by the Network Simulator 2 (NS2). We have simulated the various types of flooding attack and then attempted to detect as well as prevent it in near real time. The results have shown that our approach can be very helpful in identifying a DDoS attack and preventing it at the earliest so that the bandwidth of the network remains available to the legitimate users.

Keywords: Denial of Service (DDoS) attack, UDP Flooding , Network Simulator 2, Intrusion Prevention System