Abstract

Network security is a field of intense research and various approaches have been deployed in order to tackle network related security breaches. In this dissertation, we have worked towards the detection of DoS attacks using SNMP data. DoS attacks (Denial of Service attacks) are launched with the objective of rendering target systems inaccessible by legitimate users. Attacks that target host systems can often be checked with operating system patches. It is much more difficult, however, to defend against attacks that flood networks with data packets. Network flooding attacks can be categorized as ICMP aka Smurf, TCP SYN, UDP, TCP and combinations thereof. SNMP is protocol used for management of network. It uses MIB (Management Information Base) variables in order to manage devices (such as switches, computers, etc.) in a network. The proper selection of these variables can be used in order to detect network intrusions.

We have successfully exploited this feature of SNMP to detect different types of flood attacks in a subnet. Our algorithm provides privileges of detecting both host based as well as network based intrusions. The algorithm was successfully tested in the network system of CDAC-Bangalore, where we monitored individual hosts as well as switches. The platform used was Linux and the algorithm was developed using C.