Abstract

Nowadays secured information communication has becoming at risk. Millions of users using the Internet at any instant of time and taking full use of the application’s, services. DDoS flooding attacks are complex attempts to block the legitimate users. The Attacker normally gains access to a large number of computers by breaching their security loopholes and then they launch their attack to the target machine by these compromised machines. Intrusion Detection Systems have gained quick growth in command, scope and complexity. All IDS share an analogous primary structure: agents. Modern boost in malevolent network activity have hurried the need for IDS with global scope. A single IDS power can be grown by connecting an attack relationship engine with a database of events collected by distributed agents. This will help to provide global and single view of existing and rising attacks and will allow fast warning and ease development of countermeasures. A large number of distributed IDS with global and wide scope have been active for several years; three of these are discussed and compared with each other in this paper.
ences

- Snort (software); http://en.wikipedia.org/wiki/Snort_%28software%29
- SecTools. Org: 2006 Results; http://sectools.org/tools 20 06. html
- B. Raju1 and B. SrinivasNetwork Intrusion Detection System Using KMP Pattern
An Examination of Network Intrusion Detection System Tools and Algorithms: A Review

Matching Algorithm, IJCST, 33-36, January 2012.

Index Terms

Computer Science
Security

Keywords
DDOS  Network attacks  IDS  IDS algorithms  IDS tools