International Journal on Recent Researches In Science, Engineering & Technology
A Journal Established in early 2000 and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy.
It is an absolutely free (No processing charge No publishing charge etc) Journal Indexed in DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com
Chief Editor : 1. Dr. M.Narayana Rao, Rtd. Professor, NIT, Trichy. (Engg.&Technology division)
2. Dr. N.Sandyarani, Ph.D., Professor, Chennai based Engg.College, (Science division)

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
Volume 1, Issue 11, Nov. 2013
DIIF IF :1.46
SJIF IF: 1.329

Detection and Defense Against DDOS

B . Mopari

Abstract - It has been observed from literature that distributed Denial -of - Service (DDoS) attacks are significant problems because, they are very hard to detect , there is no comprehensive solution and it can shut an organization off from the internet . The primary goal of an attack is to deny the victims access to a particular resource. Dos is implemented using source IP address spoofing. This paper provides a framework for detecting the attack and dropping the spoofed packets. The legitimacy of a packet can be found out by analyzing the number of hops that packet gone through before reaching at the destination. Attacker can forge any field in the IP packet including TTL but he cannot control hop count. By generating an IP to Hop-Count mapping table and inspecting it , spoofed packets can be identified .HCF (Hop Count Filter) is used to classify legitimate and spoofed packets with little collateral damage. HCF causes delay in critical path of packet process in the Kernal because of enormous IP2HC mapping table. This overhead is reduced by identifying the attackers in learning state and then spoofed packets in filtering state. The PU can be reduced by implementing it in Linux Kernal in terms of interrupts.