Abstract

One of the biggest concerns for security professionals today are Distributed Denial of Service (DDoS) flooding attacks. They are nothing but explicit attempts to disrupt the legitimate users' access to services. One of the more popular DDoS attack is the SYN Flood attack. The SYN flooding attacks are launched by exploiting the TCP's three-way handshake mechanism and its limitation in maintaining its half-opened connections. The
proposal is to present a simple and robust mechanism that detects the SYN flooding attacks with less computational overhead. The two algorithms which would be used are an adaptive threshold algorithm and the cumulative sum (CUSUM) algorithm for change point detection. The proposal is to measure the performance in terms of the packet delivery fraction. The evaluation results are presented in NS2 simulation environment.

References

- J. Haggerty, Q. Shi and M. Merabti, "Early Detection and Prevention of
- L. Garber, &quot;Denial-of-Service Attack Rip the Internet&quot; Computer, April 2000.
- Netscreen 100 Firewall Appliance, http://www. netscreen . com/
- D. Moore, G. Voelker and S. Savage, &quot;Inferring Internet Denial of Service Activity&quot; Proceedings of USENIX Security Symposium 2001, August 2001

Index Terms

Computer Science

Security
Keywords
Cusum Algorithm  Ns2