AN ANALYSIS OF DDoS ATTACK METHODS, THREATS, TOOLS AND DEFENSE MECHANISMS

S. KARTHIK, V. P. ARUNACHALAM AND T. RAVICHANDRAN

Abstract

Internet has become the infrastructure of the modern society. The Internet architecture focuses on functionality and not the security. Inexperienced users leave their systems vulnerable to compromise. For example, using the vendor supplied default passwords, leaving auto-configure features in default settings, turning off firewalls, etc. makes it easy to gain root or administrator access. Distributed Denial of Service (DDoS) uses DoS as the basic building block. The main difference between DoS and DDoS attacks lies in its scale of attack and operation mode. This paper aims to provide an understanding of the existing attack methods, tools and defense mechanisms, so that a better understanding of DDoS attacks can be achieved. The goal of the paper is to simulate an environment by extending NS2, setting attacking topology and traffic, which can be used to evaluate and compare the methods of DDoS attacks and tools. Based on the simulation and evaluation results, more efficient and effective algorithms, techniques and procedures to combat these attacks may be developed.