International Journal of Innovative
Computing, Information and Control
Volume **5**, Number **3**, March **2009**

 ISSN 1349-4198
pp. 555–565

PERFORMANCE EVALUATION FOR LINUX UNDER SYN FLOODING ATTACKS

Shunsuke Oshima[1] and Takuo Nakashima[2]

[1]Information and Electronic Engineering
Yatsushiro National College of Technology
2627, Hirayama-Shinmachi, Yatsushiro, Kumamoto, Japan
oshima@as.yatsushiro-nct.ac.jp

[2]School of Industrial Engineering
Tokai University
9-1-1 Toroku, Kumamoto, Japan
taku@ktmail.tokai-u.jp

Received February 2008; revised June 2008

Abstract. *The SYN flooding attack is a DoS(Denial of Service) method affecting hosts to retain the half-open state and causing to exhaust it's memory resources. This attack is hardly filtered by routers in such a case that the source IP address is spoofed. In this paper, we present a performance evaluation for Linux platform under SYN flooding attacks. We implement an attacking and an observing program, and observe response packets from the server and the performance of system under DoS attacks. Our method explores three features for Linux. Firstly, syncookie mechanism provides the reliable first SYN+ACK response, whereas most of the SYN+ACK retransmission packets are lost. Secondly, Linux Fedra 8 improved response time without discarding the first SYN+ACK response using small cache area for half-open information. Thirdly, Linux server performance does not degrade under the DoS attacks exceeding 100,000 sequential SYN requests.*
Keywords: DDoS attack, Linux, Syncookie, Performance evaluation

1. **Introduction.** DoS attacks are easily performed by taking advantage of the weakness of the network protocol and by iterating requests of service for the application. Most organization have opened their Web sites and other ports on TCP to maintain their sites. Therefore, these attacks aim directly at the application of Web server or TCP protocol to suspend their Internet services. In a DDoS (Distributed Denial of Service) attack, the assault is coordinated across many hijacked systems by a single attacker [1]. SYN flooding attacks [2][3] disturb the establishment of the TCP connection. An attacker does not respond to the SYN+ACK packet from the server following a huge amount of SYN packets sent to the server from the attacker with spoofed source IP addresses. As a result, TCP on the server should keep the huge number of the half-open state for each connection and exhaust the memory resource to be followed by the cease of server function to be eventually down. This SYN flooding attack has been observed world-wide, and occupies approximately 90% of the DoS attacks [4].

The mechanism to prevent these flooding-based DoS/DDoS attacks is generally classified in three types; source-end defense, network-path based defense and victim-end defense, based on the network distance from attackers. To defend victims, early and precise detection mechanisms for spoofed IP addresses are required at the victim network or host. Our approach mainly focuses on the early detection mechanism for SYN flooding DDoS attacks at the victim host.