Detecting DRDoS attack by Log File based IP pairing mechanism

P.MOHANA PRIYA[1] V.AKILANDESWARI[1] S.MERCY SHALINIE[2]

Department of Computer Science and Engineering
Thiagarajar College of Engineering
Madurai – 625016, Tamil Nadu,
India
amshika11@gmail.com, akilavembu@gmail.com, shalinie@tce.edu

Abstract: - As the number of security threats and attacks increase the need for developing flexible and automated network security mechanism also increase. The main objective of this paper is to propose a Reflection Attack Log File (RALF) based IP pairing detection method to detect the TCP-SYN reflection attack. The proposed RALF based IP pairing detection method is best suitable for all the types of protocols such as TCP, UDP, ICMP packets and it belongs to the category of protocol independent detection method. The RALF based IP pairing detection method involves log files which comprises the details of source and destination addresses that are considered to be the comparative parameter for detecting the TCP-SYN reflection attack. In the experimental analysis, the performance of the proposed method is analyzed with Distributed Denial of Service (DDoS) and Distributed Reflection Denial of Service (DRDoS) attack traffic. This method achieves (99%) of True Positive Rates (TPR) and less (1%) of False Positive Rate (FPR) when compared to existing reflected attack detection method. The proposed RALF based IP pairing detection method effectively detects the TCP-SYN reflection attacks before the attack reaching the target server. The results show that the proposed RALF based IP pairing detection method detects the highest probability of attack traffic.

Key-Words: - DDoS attack, DRDoS attack, Reflection attack, TCP-SYN Reflection attack, High-rate flooding attacks, Log file.

1 Introduction

The origin of Denial of Service (DoS) attack created a very big challenge to the ever developing internet infrastructure. The intention of Denial of Service (DoS) attack [5] is to stop the requested services by the clients (or) users. The attacker takes control over a single machine in a unique network to achieve DoS attack at the target server. Later, in order to distribute the DoS attack, attacker takes control over a large of machines remotely residing in different networks. This kind of attack is termed as Distributed Denial of Service (DDoS) attack. The attacker then spreads their attack range using reflector components by directing the response packets to the target server [9]. The characteristics of DDoS and DRDoS attack traffics [8] are compared which clearly indicates that DRDoS attack created a very big challenge to the researchers as the source IP address is spoofed. This special characteristic of DRDoS attack is termed as anonymity (or) anonymous. DRDoS attacks are broadly classified as bandwidth exhaustion attacks and resource consumption attacks.

The DRDoS attacks are used to exploit the protocols such as TCP, UDP, ICMP, HTTP etc. This paper concentrates on the TCP-SYN reflection attack and its proposed RALF based IP pairing detection method to identify the TCP SYN- ACK reflected response packets. The normal working procedure of TCP involves the client sending a SYN request to the server for connection establishment. Server then acknowledges the SYN request by sending the SYN-ACK (acknowledgement for the SYN request) to the client. The client then sends the ACK (acknowledgement for the SYN-ACK packet) to the server.

The steps for an attacker to launch TCP-SYN reflection attack is divided into two parts. The first part of an attacker is to spoof the source IP address of the origin which is same as target datacenter server. In this step, the TCP-SYN request is sent to the reflector from an attacker with the destination