Real Time Detection of Application Layer DDos Attack Using Log Based Collaborative Intrusion Detection System

Authors : Farheen Tabassum, Shoab Ahmed Khan

Abstract : The brutality of attacks on networks and decisive infrastructures are on the climb over recent years and appears to continue to do so. Distributed Denial of service attack is the most prevalent and easy attack on the availability of a service due to the easy availability of large botnet computers at cheap price and the general lack of protection against these attacks. Application layer DDoS attack is DDoS attack that is targeted on wed server, application server or database server. These types of attacks are much more sophisticated and challenging as they get around most conventional network security devices because attack traffic often impersonate normal traffic and cannot be recognized by network layer anomalies. Conventional techniques of single-hosted security systems are becoming gradually less effective in the face of such complicated and synchronized multi-front attacks. In order to protect from such attacks and intrusion, corporation among all network devices is essential. To overcome this issue, a collaborative intrusion detection system (CIDS) is proposed in which multiple network devices share valuable information to identify attacks, as a single device might not be capable to sense any malevolent action on its own. So it helps us to take decision after analyzing the information collected from different sources. This novel attack detection technique helps to detect seemingly benign packets that target the availability of the critical infrastructure, and the proposed solution methodology shall enable the incident response teams to detect and react to DDoS attacks at the earliest stage to ensure that the uptime of the service remain unaffected. Experimental evaluation shows that the proposed collaborative detection approach is much more effective and efficient than the previous approaches.

Keywords : Distributed Denial-of-Service (DDoS), Collaborative Intrusion Detection System (CIDS), Slowloris, OSSIM (Open Source Security Information Management tool), OSSEC HIDS

Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development

Conference Location : Chicago, United States

Conference Dates : December 12-13, 2020

Open Science Index, Mathematical and Computational Sciences Vol:14, No:12, 2020 publications.waset.org/abstracts/23855.pdf