A Survey on Slow DDoS Attack Detection Techniques

Oluwatobi Shadrach Akanji Department of Computer Science Federal University of Technology Minna, Nigeria akanjioluwatobishadrach@yahoo.com

Opeyemi Aderiike Abisoye Department of Computer Science Federal University of Technology Minna, Nigeria o.abisoye@futminna.edu.ng

Sulaimon A. Bashir Department of Computer Science Federal University of Technology Minna, Nigeria bashirsulaimon@futminna.edu.ng

Oluwaseun Adeniyi Ojerinde Department of Computer Science Federal University of Technology Minna, Nigeria o.ojerinde@futminna.edu.ng

***Abstract*—** The ease with which DDoS attack is being launched using publicly available tools has made DDoS to be a recurring security problem. However, given the immense work by researchers to stem the tide of volumetric DDoS, attackers have resorted to using a slow DDoS attack which is similar to benign traffic thus making detection and mitigation difficult. This paper seeks to provide the scholarly community with a survey on slow DDoS attack detection techniques worked upon by researchers over time. A low amount of work has been done when the work on slow DDoS detection is juxtaposed with that of volumetric DDoS. However, researchers who have worked on detecting slow attacks have achieved remarkable results. Machine learning detection technique has proven to be effective with random forest and K-Nearest Neighbour (KNN) being the major algorithms that have consistently achieved good results in terms of Area Under Curve (AUC), accuracy, and false positive rate. Other detection techniques of time series and performance model have also been effective against slow DDoS but need to be improved upon given the non-linearly separable nature of a slow attack and benign traffic. Most researchers resorted to using attack tools to generate attack data due to the absence of a standard data set. Recommendations for future studies include exploration of detecting slow table overflow attacks in SDN before a table overflow event occurs.

Keywords—Slow DDoS, Slowloris, Slow POST, Slow Read, Slow attack detection, Slow HTTP

3rd