ABSTRAK

Keamanan jaringan komputer merupakan aspek krusial yang harus diperhatikan oleh setiap pengguna komputer untuk melindungi validitas, integritas data, dan ketersediaan layanan. Ancaman terhadap keamanan jaringan seperti serangan Distributed Deniel of Service (DDoS) dapat mengakibatkan gangguan serius pada system, kerusakan perangkat, dan gangguan layanan. Serangan DDoS yang sering digunakan adalah ping of deadth, Dimana penyerang membanjiri server target dengan paket ICMP, yang menyebabkan server menjadi lambat dan tidak responsif. Penelitian ini berfokus pada Audit Keamanan Jaringan Pada Jaringan Komputer Server menggunakan Snort Intrusion Detection System terhadap serangan DDoS ping of deadth Tujuan dari penelitian ini adalah untuk mengidentifikasi sumber serangan, waktu kejadian, aktifitas data traffic jaringan, serta dampak serangan terhadap server. Dari penelitian ini didapatkan hasil serangan ping of deadth dan flooding terhadap jaringan komputer server dengan ip 192.168.80.2 mampu membuat kinerja server menjadi lambat, terlihat dari peningkatan performance CPU Load pada perangkat jaringan server dalam keadaan normal dari 4% menjadi 100% dan memory dari 22,0MiB menjadi 22,1MiB yang menyebabkan jaringan server menjadi down. Hasil dari Penelitian ini diperoleh Snort dengan metode Intrusion Detection System efektif digunakan dalam audit keamanan jaringan komputer server dengan kemampuan mendeteksi serangan secara real time dan dapat mendeteksi waktu terjadinya penyerangan, ip penyerang, dan jenis serangan yang dilakukan secara Real Time.

Kata Kunci : Audit, Keamanan, Server, *Snort*, *Intrusion Detection System*

ABSTRACT

Computer network security is a crucial aspect that must be considered by every computer user to protect the validity, data integrity, and availability of services. Threats to network security such as Distributed Denial of Service (DDoS) attacks can cause serious system disruption, device damage, and service disruption. The most commonly used DDoS attack is ping of deadth, where the attacker floods the target server with ICMP packets, causing the server to become slow and unresponsive. This study focuses on Network Security Audit on Server Computer Networks using the Snort Intrusion Detection System against DDoS ping of deadth attacks. The purpose of this study is to identify the source of the attack, time of occurrence, network traffic data activity, and the impact of the attack on the server. From this study, the results of ping of deadth and flooding attacks on the server computer network with ip 192.168.80.2 were able to slow down server performance, as seen from the increase in CPU Load performance on the server network device in normal conditions from 4% to 100% and memory from 22.0MiB to 22.1MiB which caused the server network to go down. The results of this research obtained Snort with the Intrusion Detection System method are effective for use in server computer network security audits with the ability to detect attacks in real time and can detect the time of the attack, the attacker's IP, and the type of attack carried out in real time.

Keywords: Audit, Security, Server, Snort, Intrusion Detection System