# Monitoring jaringan dan deteksi serangan DoS pada wireless network menggunakan intrusion detection system = Network monitoring and detection of DoS attacks on wireless networks using intrusion detection system

Sherly, author



---

Abstrak

Dengan berkembangnya teknologi menyebabkan banyaknya kerentanan yang dapat terjadi pada jaringan wireless yang sering kali dimanfaatkan oleh berbagai pihak contohnya serangan DoS. Oleh karena itu sangat dibutuhkan sistem yang user friendly untuk memudahkan user dalam mendeteksi dan mencegah serangan tersebut sebelum attacker membahayakan jaringan. System tersebut dinamakan Intrusion Detection System (IDS). Pada pengujian ini menggunakan sistem operasi windows 10 dengan beberapa tools yaitu Snort sebagai IDS software, BASE sebagai report modul, Kiwi Syslog untuk menampilkan alert, dan hub sebagai network device. Ada beberapa jenis serangan yang dilakukan yaitu IP Scan dan Port Scan digunakan untuk mencari IP dan Port yang terbuka agar dapat diserang, dan Flooding sebagai penyerangnya. Dalam pengujian ini, terdapat beberapa skenario yang dilakukan yaitu pengujian Functionality Test pada client 1 – 3 untuk membandingkan nilai serangan, dan juga untuk mengetahui response time dari serangan yang dilakukan tersebut. Pada skenario pertama, dilakukan flooding pada 1 client (komputer target) dengan IP address 192.168.0.8 selama 60 menit lalu mendapatkan hasil 307.758 alert dan response time selama 0.000105741 s. Pada skenario kedua, dilakukan flooding terhadap 2 client sekaligus dengan IP address 192.168.0.1 dan 192.168.0.5 lalu hasil yang didapatkan sebanyak 378.920 alert dan response time selama 0.000127213 s. Dan pada skenario ketiga, dilakukan flooding terhadap 3 client sekaligus dengan IP address 192.168.0.8, 192.168.0.9, dan 192.168.0.4 lalu mendapatkan hasil sebanyak 430.212 alert dan response time selama 0.000142852 s. Pada setiap skenario dilakukan pengujian sebanyak 10 kali untuk melihat hasil yang didapatkan. Hasil yang didapat setelah melakukan pengujian tersebut ternyata mengalami kenaikan alert yang ditunjukan dengan persentase sebagai berikut yaitu dari skenario pertama ke skenario kedua sebesar 23,12%, skenario kedua ke skenario ketiga sebesar 13,53%, skenario pertama ke skenario ketiga sebesar 39,78%. Begitupula dengan response time yaitu dari skenario pertama ke skenario kedua sebesar 20,30%, skenario kedua ke skenario ketiga sebesar 12,29%, skenario pertama ke skenario ketiga sebesar 35,09%..... With the development of technology, it causes many vulnerabilities that can occur in wireless networks which are often exploited by various parties, for example DoS attacks. Therefore, a user friendly system is needed to make it easier for users to detect and prevent these attacks before the attacker harms the network. The system is called the Intrusion Detection System (IDS). In this test using the Windows 10 operating system with several tools, namely Snort as IDS software, BASE as a report module, Kiwi Syslog to display alerts, and a hub as a network device. There are several types of attacks carried out, namely IP Scan and Port Scan used to find IP and open ports so that they can be attacked, and Flooding as the attacker. In this test, there are several scenarios that are carried out, namely Functionality Tests on clients 1-3 to compare the attack values, and also to determine the response time of the attacks carried out. In the first scenario, one client (target computer) was flooded with the IP address 192.168.0.8 for 60 minutes and then got 307.758 alerts and 0.000105741 s response time. In the second scenario, 2 clients are flooded at once with IP

addresses 192.168.0.1 and 192.168.0.5 then the results obtained are 378,920 alerts and response time is 0.000127213 s. And in the third scenario, 3 clients are flooded at once with IP addresses 192.168.0.8, 192.168.0.9, and 192.168.0.4 and then get 430,212 alerts and a response time of 0.000142852 s. In each scenario, 10 times were tested to see the results obtained. The results obtained after carrying out the test turned out to have increased alerts as indicated by the following percentages, namely from the first scenario to the second scenario of 23.12%, the second scenario to the third scenario of 13.53%, the first scenario to the third scenario of 39.78 %. Likewise, the response time from the first scenario to the second scenario is 20.30%, the second scenario to the third scenario is 12.29%, the first scenario to the third scenario is 35.09%.