

ABSTRAK

HIDS (*Host based Intrusion Detection System*) adalah salah satu jenis IDS (*Intrusion Detection System*) yang berjalan pada *host* yang berdiri sendiri atau perlengkapan dalam sebuah jaringan. Sebuah HIDS melakukan pengawasan terhadap paket-paket yang berasal dari dalam maupun dari luar hanya pada satu alat saja dan kemudian memberi peringatan kepada *user* atau *administrator* sistem jaringan akan adanya kegiatan-kegiatan yang mencurigakan yang terdeteksi oleh HIDS. DDOS menggunakan banyak host penyerang, untuk menyerang satu host target. Perbedaan dengan serangan DOS biasa, apabila serangan DOS bersifat "satu lawan satu", maka untuk DDOS ini menjadi "satu lawan Banyak", sehingga pertahanan *host* target akan lebih mudah dijebol dan dibanjiri *traffic* sehingga membuat *server host* menjadi *down* dan tidak bisa diakses penggunaannya. Dengan HIDS, *administrator* jaringan akan semakin mudah mencegah serangan DDOS. Pada *functionality* HIDS mampu mendeteksi beberapa variasi serangan yaitu *ICMP flood*, *TCP flood*, dan *UDP flood*. Berdasarkan percobaan yang telah dilakukan *rules* snort dapat dibuat dengan melakukan perbandingan antara data dari *client* dan data dari penyerang. Berdasarkan percobaan yang telah dilakukan terjadi kenaikan *response time* atau lambatnya *response time* ketika paket data yang dikirim lebih kecil. Ini disebabkan *rules* snort harus menganalisa paket data yang masuk dalam jangka waktu tertentu agar tidak terjadi *false alarm*.

Kata Kunci: HIDS (*Host Based Intrusion Detection System*), SNORT, DDOS (*Distributed Denial Of Service*)

ABSTRACT

HIDS (*Host -based Intrusion Detection System*) is one kind of IDS (*Intrusion Detection System*) running on a stand-alone host or equipment in a network . A HIDS monitors the packets that come from within and from outside only on one device and then warn the user or administrator of the network system of the existence of suspicious activities are detected by a HIDS . DDOS attacker uses many hosts to attack a target host . The difference with the usual DOS attack , if a DOS attack is " one on one " , then to the DDOS be " one-to- Many " , so that the target host defenses will be more easily hacked and flooded with traffic to make the host server to be down and inaccessible users . With HIDS , network administrators will be easier to prevent DDOS attacks . In HIDS functionality capable of detecting multiple variations that ICMP flood attack , TCP flood , and UDP flood . Based on experiments that have been conducted Snort rules can be created by making a comparison between the data from the client and the data from attackers . Based on experiments that have been conducted an increase in response time or slow response time when data packets are sent smaller . This is due to snort rules should analyze incoming data packets in a certain period in order to avoid false alarms.

Keywords: HIDS (*Host Based Intrusion Detection System*), SNORT, DDOS (*Distributed Denial Of Service*)