

PLAGIAT MERUPAKAN TINDAKAN TIDAK TERPUJI

ABSTRAK

Keamanan merupakan salah satu hal yang diperlukan ketika sedang melakukan suatu kegiatan. Dengan adanya rasa aman yang terjamin, kegiatan yang sedang dialakukan bisa berjalan dengan lancar tanpa adanya rasa takut. Begitu pula dengan keamanan pada jaringan komputer yang dibutuhkan ketika sedang menggunakan komputer yang terhubung dengan koneksi internet. Ancaman terhadap keamanan jaringan komputer selalu ada, tetapi ancaman tersebut dapat diatasi apabila serangan tersebut bisa diketahui terlebih dahulu dengan menggunakan *Intrusion Detection System* atau IDS. IDS *open source* yang popular adalah Snort. Selain Snort ada IDS *open source* yang juga memiliki kemiripan dengan Snort, yaitu Suricata yang masih tergolong baru.

Untuk membandingkan kemampuan pendekripsi antara Snort dan Suricata, penulis menggunakan perangkat keras yang sama. Pengujian dilakukan dengan melakukan percobaan serangan menggunakan *tools* pengujian bernama Pytbull. Serangan yang digunakan adalah sama, yaitu dengan serangan dan jumlah serangan yang sama.

Dari hasil pengujian, diperoleh hasil yaitu Snort dapat mendekripsi lebih banyak daripada Suricata meskipun menggunakan sumber daya komputer yang sedikit. Sedangkan Suricata, meskipun masih tergolong baru, juga dapat mendekripsi percobaan serangan yang dilancarkan oleh Pytbull meskipun membutuhkan sumber daya komputer yang lebih banyak daripada Snort.

Kata Kunci :Keamanan, IDS, Snort, Suricata, Pytbull

PLAGIAT MERUPAKAN TINDAKAN TIDAK TERPUJI

ABSTRACT

Security is one of the things that are required when doing an activity. With their sense of security is assured, activities underway could run smoothly without any fear. Similarly, the security of the computer network is required when using a computer connected to the internet connection. Threats to the security of computer networks have always existed, but the threat can be overcome if the attack can be known in advance by using Intrusion Detection System or IDS. The popular open source IDS is Snort. In addition there Snort open source IDS which also has similarities with Snort, that Suricata is still relatively new.

To compare the detectability between Snort and Suricata, the author uses the same hardware. Testing is done by experimenting attacks using testing tools called Pytbull. The attack used is the same, namely the attack and the number of the same attack.

From the test results, obtained results that Snort can detect more than Suricata despite using little computer resources. While Suricata, although still relatively new, it can also detect attempted attacks launched by Pytbull although it requires more computer resources than Snort.

Keyword : Security, IDS, Snort, Suricata, Pytbull