ABSTRACT

Intrusion Detection System is is one of the computer network security infrastructure that analyzes the packets across the network to detect possible intrusion. Typically, IDS is used and has evolved into newer approaches such as the use of the method signature and anomaly. Signature method is preferred because it has several advantages than the more advanced methods of anomaly. Many methods signatures have been developed, and one of them is based on the Generation Automated Rules, where this method utilizes honeypot server to be manufacture IDS rules-based logs of honeypot. Some of the drawbacks of the Rules Generation Automated methods used today are less able to detect network attacks and less efficient in its use.

In this study, new methods are used to make improvements to existing Generation Automated Rules methods, the method used is to eliminate redundant data, and reduce the number of rules that have similarities, the number of rules generated from log honeypot can be reduced, so that the performance of detection Snort is more efficient and better in terms of detection accuracy than existing methods. In this study, the method used is automated generation rules which is the method of making the Snort rules derived from the server honeypot log, which is then processed further manually to generate the Snort rules.

The results show that the proposed method has better detection rates when compared to the use of Apriori algorithms and standard Automated Generation Rules methods, but with more efficient use of resources. The proposed method is 19.52% faster than Conventional methods, less in memory usage of 0.64% than Apriori methods, and 72.96% less than conventional methods.

Keywords : snort, honeypot, automatic generations rules.

INTISARI

Intrusion Detection System adalah infrastruktur keamanan jaringan komputer yang menganalisis paket pada jaringan untuk mendeteksi kemungkinan gangguan intrusi. IDS telah banyak berevolusi menjadi pendekatan yang baru seperti penggunaan metode *signature* dan *anomaly*. Metode *signature* lebih banyak digunakan di dalam industri keamanan karena memiliki beberapa kelebihan dibanding metode *anomaly*. Banyak metode *signature* telah dikembangkan, salah satunya yaitu metode *Generated Automated Rules*, metode yang memanfaatkan *log honeypot* untuk membuat *rules* Snort. Metode Generasi Otomatis yang digunakan saat ini kurang masih menyisakan kelmahan yaitu dalam deteksi dan kurang efisien dalam penggunaan sumber daya sistem.

Pada penelitian ini, metode baru digunakan untuk melakukan perbaikan pada metode *Generation Automated Rules* yang sudah ada, metode yang digunakan yaitu dengan menghilangkan data yang redundant, serta mengurangi jumlah *rules* yang memiliki kesamaan, jumlah rules yang dihasilkan dari *log honeypot* dapat dikurangi, sehingga performa deteksi Snort lebih efisien dan lebih baik dalam hal akurasi deteksi dari metode yang sudah ada. Pada penelitian ini, metode yang digunakan yaitu *automated generation rules* yang merupakan metode pembuatan *rules* Snort berasal dari *log honeypot server*, yang kemudian diproses lebih lanjut secara manual untuk menghasilkan *rules* Snort.

Hasil penelitian menunjukkan bahwa metode yang diusulkan memiliki tingkat deteksi yang lebih baik jika dibandingkan dengan penggunaan algoritme Apriori dan metode *Autoated Generation Rules* standar, namun dengan penggunaan sumber daya yang lebih efisien. Metode yang diusulkan lebih cepat 19,52% dari metode Konvensional, lebih sedikit dalam penggunaan memori 0,64% dari metode Apriori, dan lebih sedikit 72,96% daripada metode konvensional.

Kata kunci -- ids, snort, pembangkitan aturan otomatis.