INTISARI

PERBANDINGAN KINERJA SNORT DAN SURICATA SEBAGAI SISTEM PENDETEKSI INTRUSI

Muhammad Fauzan Dzulqarnain
10/305246/PA/13467

Keamanan menjadi salah satu faktor penting yang mulai diperhatikan saat akan membangun jaringan komputer. *Intrusion detection system* atau sistem pendeteksi intrusi merupakan salah satu usaha yang dikembangkan untuk tujuan melindungi sistem. Dua *tools* yang banyak digunakan dalam usaha membangun sistem pendeteksi intrusi adalah Snort dan Suricata.

Pada penelitian ini dilakukan perbandingan terhadap kinerja kedua *tools* pembangun sistem pendeteksi intrusi tersebut dengan menggunakan serangan *scanning* berupa *Quick scan* dan *Intense scan* dari Zenmap serta serangan DoS dari Xerxes. Parameter yang dibandingkan diantaranya meliputi banyaknya kejadian yang berhasil terdeteksi, lamanya waktu pemindaian yang dibutuhkan, serta banyaknya paket data yang berhasil dikirim.

Dari hasil penelitian didapatkan bahwa Snort IDS lebih unggul daripada Suricata IDS saat diberikan serangan *scanning* oleh Zenmap, baik *Quick scan* maupun *Intense scan*. Tetapi, keduanya menunjukkan tingkat kinerja yang sama saat diberikan serangan DoS oleh Xerxes.

Kata kunci: Sistem pendeteksi intrusi, *Intrusion Detection System*, IDS, Snort, Suricata.

ABSTRACT

PERFORMANCE COMPARISON OF SNORT AND SURICATA AS INTRUSION DETECTION SYSTEM

Muhammad Fauzan Dzulqarnain
10/305246/PA/13467

Security becomes an important factor that began to be noticed when a computer network was built. Intrusion detection system is one of the ways which was developed for the purpose of protecting the computer system. Snort and Suricata are the most used tools to built an intrusion detection system.

A performance comparison between the tools was done in this research using scanning attacks such as Quick scan and intense scan from Zenmap and DoS attack from Xerxes. The parameters in this comparison comprised the number of events that successfully detected, the scanning time, and the amount of data packets that was successfully sent.

The result shows that Snort IDS is better than Suricata IDS when the scanning attack was given by Zenmap, both Quick scan and Intense scan. Though, both of them shows the same performance level when the DoS attack is given by Xerxes.

Keyword: Intrusion Detection System, IDS, Snort, Suricata.