Perancangan dan Analisis Kinerja Intrusion Detection System (IDS) Suricata serta Integrasi dengan sistem Keamanan Jaringan Komputer Berbasis Web = Design and Performance Analysis of Suricata Intrusion Detection System (IDS) and Integration with Web-Based Computer Network Security System

Muhammad Hafidz, author

Abstrak

Semakin berkembang atau baru teknologi yang digunakan, maka semakin banyak pula kerentanan yang muncul terhadap keamanan tersebut. Oleh karena itu pembaharuan keamanan jaringan penting untuk dilakukan secara rutin. Sebagai pemilik jaringan komputer atau biasa disebut administrator, keamanan jaringan merupakan hal yang penting untuk diperhatikan, baik itu dalam jaringan skala besar maupun kecil. Salah satu hal yang dapat dilakukan untuk meningkatkan keamanan jaringan adalah dengan melakukan perlindungan terhadap aktivitas yang mencurigakan dalam suatu jaringan dengan menggunakan teknologi yang sudah ada. Terdapat teknologi yang menyediakan fungsi untuk melakukan pencegahan dan pendeteksian terhadap aktivitas mencurigakan tersebut, dinamakan Intrusion Detection System (IDS), khususnya yang berbasis Host. IDS berfungsi untuk meningkatkan keamanan suatu jaringan atau host dengan cara melakukan pendeteksian serta pencocokan packet pada traffic hingga menemukan suatu ancaman yang terdeteksi. Selanjutnya IDS akan dibantu oleh ELK Stack untuk memvisualisasikan kumpulan dari ancaman yang terdeteksi serta memberikan alert dengan waktu yang cepat. Visualisasi ancaman dan alert akan diolah dan ditampilkan pada aplikasi web berbentuk dasbor, sehingga lebih mudah dipahami oleh Administrator Jaringan sehingga Administrator dapat mengambil tindakan yang paling efektif untuk mencegah dan mengurangi kerusakan yang diakibatkan ancaman tersebut. Pada penelitian ini digunakan IDS Suricata yang bersifat Open Source dengan menggunakan rule “Emerging Threat Open Ruleset”, serta pengolahan log dan visualisasi dengan Elasticsearch, Logstash dan Kibana (ELK) Stack. IDS Suricata telah terkonfigurasi dengan baik dan dapat mendeteksi seluruh skenario penyerangan dengan akurasi 64%. Integrasi dengan ELK berhasil dilakukan dengan data alert telah ditampilkan pada dasbor Kibana. Pada saat terjadi serangan, sumber daya pada IDS mengalami peningkatan, dengan hasil 54.3% untuk SYN Flood, 5.5% untuk IP Scanning, dan 5.8% untuk Intense Port Scan. Sedangkan 3.26GB memori digunakan untuk SYN Flood, 3.15GB untuk IP Scanning dan 3.22GB untuk Intense Port Scan.
.....The rapid development of technology, especially in information technology, forces all technology users to always get the latest information and implement existing technology with the latest technology. Similarly, technological developments in the field of security, especially in computer network security. The more developed or new the technology is used, the more vulnerabilities that arise against this security. Therefore, it is important to update network security regularly. As a computer network owner or commonly called an administrator, network security is an important thing to put attention to, both in large and small scale networks. One of the things that can be done to improve network security is to protect against suspicious activity in a network or in a host/server using existing technology. There is a technology that provides functions to prevent and detect such suspicious activity, called the Intrusion Detection System (IDS), especially Host Based IDS. IDS serves to improve the security of a network by detecting and matching

traffic to find a detected threat. Furthermore, the IDS will be assisted by the ELK Stack to visualize the collection of detected threats and provide alerts in a fast time. Visualization of threats and alerts will be processed and displayed on a web application in the form of a dashboard, making it easier for network administrators to understand so that administrators can take the most effective action to prevent and reduce damage caused by these threats. This research uses IDS Suricata which is Open Source by using the "Emerging Threat Open Ruleset" rule, as well as log processing and visualization with Elasticsearch, Logstash and Kibana (ELK) Stack. The configured Suricata IDS is able to detect all attacks that occur with 64% Accuracy, and integration with ELK can be done with the data displayed on the Kibana dashboard. The use of additional resources on the computer is 54.3% for SYN Flood, 5.5% for IP Scanning, and 5.8% for Intense Port Scan. Meanwhile, 3.26GB of memory is used for SYN Flood, 3.15GB for IP Scanning, and 3.22GB for Intense Port Scan.