Implementasi Intrusion Detection System Menggunakan Zeek dan Suricata untuk Network Monitoring melalui SIEM Dashboard = Implementation of Intrusion Detection System using Zeek and Suricata for Network Monitoring through a SIEM Dashboard

Theodorus Lucas, author

Abstrak

Penelitian ini melakukan implementasi dan perbandingan performa antara tools Suricata dan Zeek sebagai IDS yang diintegrasikan dengan SIEM dashboard menggunakan ELK stack. Tujuan dari penelitian ini ialah untuk menunjukkan implementasi dari kedua tools ini untuk mendukung kegiatan network monitoring, dan juga mengukur performa dari masing-masing tools sebagai IDS dalam menghadapi serangan siber berupa denial-of-service (DoS). Penelitian ini dilakukan di dalam sebuah jaringan internal, dengan menggunakan server Linux untuk IDS maupun ELK stack. Pengujian yang dilakukan berupa pengujian tiga buah skenario, yang masing-masing mensimulasikan jenis serangan DoS yang berbeda. Terdapat dua aspek penilaian performa, yaitu performa angka persentase deteksi dan juga angka persentase penggunaan sumber daya CPU dan memori. Hasil yang diperoleh menunjukkan bahwa sebagai IDS, Suricata lebih diunggulkan dibandingkan Zeek karena dashboard yang lebih beragam dan memiliki fitur alerting; memiliki persentase deteksi yang lebih besar untuk dua dari tiga skenario yang diujikan, yaitu sebesar 86,14% untuk skenario 1 dan 79,41% untuk skenario 3; dan juga memiliki penggunaan sumber daya yang lebih efisien dari seluruh skenario yang diujikan, yaitu penggunaan CPU dan memori masing-masing sebesar 24,32% dan 3,88% untuk skenario 1, 29,12% dan 4,56% untuk skenario 2, serta 16,96% dan 4,66% untuk skenario 3.
.....This research conducts the implementation and performance comparison between Suricata and Zeek tools as an IDS integrated with a SIEM dashboard using the ELK stack. The aim of this study is to demonstrate the implementation of both tools to support network monitoring activities and measure the performance of each tool as an IDS in facing denial-of-service (DoS) cyber attacks. The research was conducted within an internal network, utilizing Linux servers for both IDS and the ELK stack. The testing involved three scenarios, each simulating different types of DoS attacks. There are two performance evaluation aspects: detection rate (DR) performance and CPU and memory resource utilization rate. The results indicate that Suricata is favored over Zeek as an IDS due to its more enhanced dashboard and better alerting features; a better DR for two of the three scenarios tested, with DR values of 86,14% for scenario 1 and 79,41% for scenario 2; and also more efficient resource usage for all three scenarios tested, which for CPU and memory usage respectively is 24,32% and 3,88% for scenario 1, 29,12% and 4,56% for scenario 2, and 16,96% and 4,66% for scenario 3.