Sistem Security Information & Event Management (SIEM) untuk Live Analysis berbasis Machine Learning pada Intrusion Detection System (IDS)

Adabi Raihan Muhammad[1], Parman Sukarno, ST, M.Sc, Ph.D [2], Aulia Arif Wardana, S.Kom., M.T. [3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]adabiraihanm@students.telkomuniversity.ac.id, [2]psukarno@telkomuniversity.ac.id,
[3]auliawardan@telkomuniversity.ac.id

Abstrak

Penerapan Intrusion Detection System (IDS) dengan menggunakan teknik *machine learning* yang terintegrasi dengan Security Information & Event Management (SIEM) pada jaringan berskala besar akan meningkatkan keamanan jaringan karena sistem IDS berbasis machine learning dapat mendeteksi anomali pada setiap paket yang dinilai dari aktivitas paket di jaringan tersebut sehingga dapat mengurangi terjadinya serangan pada jaringan, dibandingkan dengan menggunakan IDS berbasis *signature-based* dan berbasis *rule-based* yang tidak dapat beradaptasi dengan setiap paket yang dideteksi oleh IDS. Dalam jurnal ini, mengusulkan sistem yang menggabungkan 3 proyek *open-source* yaitu IDS, *Machine Learning*, dan SIEM menjadi satu dan hasil tes performansi dari sistem yang diusulkan berkinerja baik dalam pengujian DoS selama 1 jam dengan mengirimkan paket sebanyak 344.1/detik untuk menguji apakah sistem dapat bekerja optimal saat terjadinya DoS. Hasil monitoring sistem dari 4 komponen yang terdiri dari ELK Stack (Elasticsearch, Logstash, Kibana), dan Zeek (IDS) yang dimonitor untuk melihat penggunaan sistem saat sistem di DoS. Elasticsearch adalah komponen yang paling banyak menggunakan kinerja sistem dengan rincian sebagai berikut, penggunaan CPU 78% dan penggunaan RAM 2300 MB, dan penggunaan sistem yang paling sedikit dikonsumsi adalah Zeek dengan penggunaan CPU 3,5% dan penggunaan RAM 225 MB.

Kata kunci : IDS, Machine Learning, SIEM, Live Analysis