Deteksi Duplicate Session pada Sistem Informasi Berdasarkan Klasifikasi IP Public dalam Pencegahan Joki Online

Yessy Fitriani [1]; M. Yoga Distra Sudirman [2]; Dine Tiara Kusuma [3], Christ Stefanie Siburian [4]

[1,2,3,4] Institusi Teknologi PLN

yessy.fitriani@itpln.ac.id

ABSTRAK

Salah satu jenis proteksi serangan sistem informasi adalah sistem deteksi intrusi yang dikombinasikan dengan analisis data log. Setiap aktifitas akan dipantau (logging) kemudian sistem deteksi intrusi menganalisis log tersebut dan mencoba untuk menemukan aktifitas yang tidak biasa. Tentu saja, sistem tidak dapat mencegah serangan itu, namun dapat memberikan peringatan dini agar serangan tersebut bisa segera dihentikan dan kerusakan total dapat dihindari (Liebenow, 2019).

Insiden unauthorized access menjadi salah satu ancaman bagi sistem informasi di suatu perusahaan termasuk di Institut Teknologi PLN. Kehilangan data penting, pencurian data rahasia dan pembajakan akun merupakan beberapa dampak yang timbul dari adanya unauthorized access seperti adanya aktifitas KRS Online mahasiswa yang dilakukan oleh Joki Online. Sistem deteksi login yang diintegrasikan dengan sistem informasi ITPLN dapat menjadi ekstensi tambahan dalam mencegah terjadinya insiden unauthorized access. Log login secara otomatis dihasilkan oleh sistem informasi dan sistem deteksi login bekerja dengan membaca data log login secara berkala serta deteksi duplikasi session berdasarkan klasifikasi IP Public. Dengan menggunakan algoritma Gaussian Naive Bayes (GNB), sistem deteksi login mampu melakukan klasifikasi dan pelatihan secara real-time. Berdasarkan hasil perhitungan confusion matrix pada skenario offline learning, diperoleh nilai akurasi sebesar 93%

Kata Kunci : Sistem Informasi, Deteksi, Login, Naïve Bayes, Serangan, Kejahatan Cyber