PREDIKSI POLA KECENDERUNGAN PENYERANGAN WEB SERVER

(STUDI KASUS : tif.uin-suska.ac.id)

MOHD. IRWAN

11251103152

Tanggal Sidang: 25 Oktober 2017

Periode Wisuda : Febuari 2018

Jurusan Teknik Informatika

Fakultas Sains dan Teknologi

Universitas Islam Negeri Sultan Syarif Kasim Riau

ABSTRAK

Log merupakan suatu file yang berisi data atau informasi mengenai seluruh aktifitas pada server baik yang ditimbulkan dari server maupun client aktifitas berupa client mengakses keserver yang menyebabkan error atau aktifitas biasa. Log tif.uin-suska.ac.id terdapat daftar tindakan, penyerangan terhadap log file web server di UIN SUSKA sehingga dapat mengantisipasi apabila ada pengunjung yang mencoba melakukan penyerangan (anomaly detection). Dengan semakin banyaknya data log, terdapat record pada log yang tidak terkait dengan proses serangan, record tersebut disebut dengan false alarm. Untuk mengurangi false alarm yang disebabkan banyaknya data log, maka akan dilakukan filtering dan statistik terhadap log menggunakan metode hidden markov models. Data yang diperoleh sebanyak 728031 baris log terdapat 405591 baris log GET respon code normal dan 39066 baris log respon kode yang dapat di *observasi*, dan data yang diperoleh dari log website tif.uin-suska.ac.id yang teramati mulai dari tanggal 20 januari sampai dengan 3 agustus 2016, dari penelitian ini diperoleh error 500 sebesar 0.002 %, 404 sebesar 8.93 %, 403 sebesar 1.31 % dari jumlah data keseluruhan dengan *precision* 53 % serta *recall* 82 % dan pola kecenderungan penyerangan, yaitu kecenderungan error berbanding lurus dengan jumlah kunjungan yang menyebabkan error.

Kata Kunci : Penyerangan, Log, IP Address, Hidden Markov Model, Website