MEMPREDIKSI SERANGAN PADA SIM (*SECURITY INFORMATION MANAGEMENT*) DENGAN MENGGUNAKAN ALGORITMA *HIDDEN MARKOV MODEL*

Rico Andreas

1610511080

Abstrak

Website merupakan suatu aplikasi yang mudah diakses dimanapun dan kapanpun, dalam kemudahan tersebut terdapat suatu serangan yang dapat dilakukan pada *website* yang tertuju langsung pada *web server*. Serangan-serangan tersebut memiliki ancaman yang sudah didata oleh OWASP (*Open Web Application Security Project*) pada tahun 2017 sehingga menciptakan informasi yang ada pada OWASP Top 10 Security – 2017 yang khusus pada aplikasi *web*. Dengan ancaman-ancaman tersebut penelitian ini dilakukan untuk membuat sistem yang dapat mendeteksi suatu serangan yang terjadi pada *website* khususnya pada *web server* dan dapat memantau serta menampilkan informasi kegiatan yang ada pada *web server* dengan *client*. *Security Information Management* (SIM) akan membaca data *access log* dan *error log* yang telah dicatat oleh *web server* lalu data tersebut akan dilakukan *training* dan *testing* dengan menggunakan algoritma *Hidden Markov Model* sehingga mendapat suatu model *learning* bagi sistem untuk mendeteksi sebuah serangan, serta *access log* dan *error log* akan diterjemahkan menjadi suatu informasi yang mudah dibaca oleh *sysadmin* kedalam suatu *dashboard*. Penelitian ini diharapkan dapat menghasilkan suatu model yang dapat mendeteksi sekaligus memantau kegiatan *web server* dalam sebuah serangan.

Kata kunci: ***Access log*****,** ***Error log*****,** ***Security Information Management,*** **SIM,** ***Hidden Markov Model***

PREDICTING AN ATTACK TO SIM (SECURITY INFORMATION MANAGEMENT) USING HIDDEN MARKOV ALGORITHM MODEL

Rico Andreas

1610511080

Abstract

Website is an app that is easily accessed anywhere and anytime, in the ease there is an attack by hackers that can be carried out on a website that is directed directly to the web server. These attacks have threats that have been recorded by OWASP (Open Web Application Security Project) in 2017 thus creating information on OWASP Security 10 - 2017 specifically on web applications. With these threats, this research was conducted to create a system that can detect an attack that occurs on a website, especially on a web server and can monitor and display information on existing activities on a web server with a client. Security Information Management (SIM) will read access log and error log data that have been recorded by the web server and then the data will be conducted training and testing using the Hidden Markov Model algorithm so that it gets a learning model for the system to detect an attack, as well as access logs and error log will be translated into information that is easily read by sysadmin into a dashboard. This research is expected to produce a model that can detect and monitor web server activities in an attack.

Keywords: Access log, Error log, Security Information Management, SIM, Hidden Markov Model