IMPLEMENTASI *INTRUSION DETECTION SYSTEM* (IDS) MENGGUNAKAN METODE *SIGNATURE RULES* PADA *DATA CENTER* UPA TIK UNDIKSHA

Oleh

Gede Beny Indrawan, NIM 1915101002

Program Studi Ilmu Komputer

Jurusan Teknik Informatika

ABSTRAK

Data center merupakan fasilitas untuk mengelola, menyimpan dan memproses jumlah data serta informasi dalam keperluan mendukung berbagai layanan dan aplikasi. Untuk memastikan keamanan dalam menjaga data pengguna UPA TIK UNDIKSHA memerlukan sistem yang dapat mendeteksi sebuah ancaman atau aktivitas mencurigakan dalam menjaga keamanan data mahasiswa, staf pegawai dan dosen. Setelah melakukan observasi dan wawancara kepada staf pegawai divisi jaringan dan keamanan, sistem deteksi intrusi memang sangat diperlukan untuk mengatasi masalah tersebut. Jadi sistem yang akan di implementasikan adalah *intrusion detection system* dengan aplikasi suricata dan menggunakan metode basis *signature-rules*. Tipe serangan yang dianjurkan untuk melakukan simulasi serangan sebelum di implementasikan pada server UPA TIK UNDIKSHA adalah serangan *web application security risks* dan serangan XSS (*Cross-Site Scripting*), karena serangan ini sering terjadi pada server UPA TIK. Proses konfigurasi suricata menggunakan basis *networking* atau NIDS (*Network-Based Intrusion Detection System*), hal ini bertujuan untuk tidak mengganggu jalur *traffic* yang dilalui server. IDS suricata dibantu dengan adanya sistem SIEM (*Security Information and Event Management*) elasticsearch untuk memantau setiap *log* atau *event* yang terjadi ketika ada peringatan serangan. Hasil yang didapatkan suricata setelah melakukan pengujian, berhasil mendeteksi serangan tanpa mengganggu *traffic* jaringan server.

Kata Kunci : *Intrusion Detection System*, Suricata, *Data Center*, *Security*, Elasticsearch

IMPLEMENTATION OF INTRUSION DETECTION SYSTEM (IDS) USING SIGNATURE RULES METHOD AT UPA TIK UNDIKSHA DATA CENTER

By

Gede Beny Indrawan, NIM 1915101002

Computer Science Study Program

Informatics Engineering

ABSTRACT

The data center is a facility for managing, storing and processing the amount of data and information in the need to support various services and applications. To ensure security in maintaining user data UPA TIK UNDIKSHA requires a system that can detect a threat or suspicious activity in maintaining the security of student data, employee staff and lecturers. After conducting observations and interviews with staff employees of the network and security division, an intrusion detection system is indeed very necessary to overcome these problems. So the system that will be implemented is an intrusion detection system with the suricata application and uses the signature-rules base method. The types of attacks recommended to simulate attacks before being implemented on the UPA TIK UNDIKSHA server are web application security risks and XSS (Cross-Site Scripting) attacks, because these attacks often occur on the UPA TIK server. The suricata configuration process uses a networking base or NIDS (Network-Based Intrusion Detection System), this aims not to interfere with the traffic path through the server. Suricata IDS is assisted by the SIEM (Security Information and Event Management) elasticsearch system to monitor every log or event that occurs when there is an attack warning. The results obtained by Suricata after testing, managed to detect attacks without disrupting server network traffic.

Keywords: Intrusion Detection System, Suricata, Data Center, Security, Elasticsearch