INTISARI

PROYEK AKHIR

PERBANDINGAN SISTEM IDPS SURICATA DALAM MODE PROMISCUOUS DAN INLINE UNTUK MERANCANG SISTEM *MONITORING* KEAMANAN JARINGAN DI PT HUTAMA KARYA

PT Hutama Karya merupakan Badan Usaha Milik Negara (BUMN) yang bergerak di bidang jasa konstruksi, pengembang dan penyedia jasa jalan tol, sehingga perusahaan menyimpan banyak data sensitif terkait proyek maupun data-data sensitif lainnya yang rentan dicuri. Untuk memblokir serangan dan pencurian data, diperlukan suatu sistem yang dapat memantau serta memblokir serangan tersebut. Salah satu sistem keamanan yang dapat digunakan untuk melindungi lalu lintas yang keluar masuk jaringan perusahaan adalah dengan menggabungkan *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS). Tujuan dari IDS adalah untuk mendeteksi aktivitas mencurigakan dalam sebuah sistem atau jaringan. Jika ditemukan aktivitas yang mencurigakan, maka IDS akan memberikan sebuah peringatan. Sedangkan IPS memiliki tujuan untuk secara otomatis memantau dan merespons ancaman yang berhasil di deteksi.

Suricata adalah perangkat lunak *opensource* yang berkerja sebagai IDS, IPS, dan *Monitoring engine* untuk keamanan jaringan yang dikelola oleh yayasan *non-profit*, Open Information Security Foundation (OISF) (Shofia, 2019). Suricata merupakan *Network-based Intrusion Detection System* (NIDS), yakni semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk ditentukan apakah ada percobaan serangan atau penyusup ke dalam sistem jaringan. NIDS diletakkan di dalam segmen jaringan penting dimana server berada atau diletakkan pada “pintu masuk” jaringan (Sundun, 2017). Suricata memiliki fungsi untuk memantau lalu lintas yang masuk dan keluar jaringan, sehingga dapat menghentikan lalu lintas berbahaya sebelum memasuki jaringan, memperingatkan Admin jaringan akan bahaya tersebut, juga dapat berfungsi untuk memblokir serangan.

Pada sistem ini, Suricata akan bekerja dengan metode *Signature-based detection* yang berkerja dengan cara mencocokkan lalu lintas jaringan dengan *rule* yang ada dan membandingkan cara kerja Suricata yang berjalan dalam Mode Promiscuous dan Inline. Pada Mode Promiscuous, lalu lintas jaringan akan di "mirror" oleh Switch Mikrotik ke Server Suricata untuk melakukan pencocokan dengan basis data yang berisi informasi serangan dan penyusupan yang telah diketahui polanya. Sedangkan pada Mode Inline, lalu lintas jaringan akan langsung melalui Server Suricata terlebih dahulu sebelum masuk ke jaringan LAN. Setelah berhasil mencocokkan ancaman dengan *rules*, Suricata akan melakukan *drop* paket mencurigakan tersebut dan Admin akan mendapat notifikasi melalui Telegram dan dapat di *Monitoring* melalui Elasticsearch dan Kibana.

Kata Kunci: *Suricata, IDPS, Elasticsearch, Kibana, Network Security*

ABSTRACT

COMPARISON OF SURICATA IDPS SYSTEM IN PROMISCUOUS AND INLINE MODE TO DESIGN A NETWORK SECURITY MONITORING SYSTEM IN PT HUTAMA KARYA

PT Hutama Karya is a State-Owned Enterprise (BUMN) which is engaged in construction services, developers, and toll road service providers. Thus, the company stores a lot of sensitive data related to projects and other sensitive data that is vulnerable to being stolen. To prevent attacks and data theft, we need a system that can monitor and prevent these attacks. One of the security systems that can be used to protect traffic coming in and out of a corporate network is to combine an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS). The purpose of an IDS is to detect suspicious activity in a system or network. If suspicious activity is found, the IDS will generate a warning. While IPS has a goal to automatically monitor and respond to threats that are successfully detected.

Suricata is opensource software that works as an IDS, IPS, and Monitoring engine for network security managed by a non-profit foundation, Open Information Security Foundation (OISF) (Shofia, 2019). Suricata is a Network-based Intrusion Detection System (NIDS), where all traffic flowing into a network will be analysedto determine whether there is an attempted attack or intruder into the network system. NIDS is placed in a critical network segment where the server is located or is placed at the "entrance" of the network (Sundun, 2017). Suricata has a function to monitor traffic entering and leaving the network, so it can stop malicious traffic before it enters the network, warn network Admins of these dangers, can also serveto prevent attacks.

In this system, Suricata will work with a Signature-based detection method that works by matching network traffic by comparing how Suricata works in Promiscuous and Inline modes. In Promiscuous mode, network traffic will be "mirrored" by the Mikrotik Switch to the Suricata Server to match the database

and rules that contains information about attacks and intrusions with known patterns. While in Inline mode, network traffic will go directly through the Suricata Server first before entering the LAN network. After successfully matching the threat to the rules, Suricata will drop the suspicious package and the Network Administrator will receive a notification via Telegram and can be monitored via Elasticsearch and Kibana.

Keywords: *Suricata, IDPS, Elasticsearch, Kibana, Network Security*