INTISARI

PERANCANGAN METODE *PROFILING* PADA *HONEYPOT INDICATOR OF COMPROMISE* (IOC) BERBASIS KORELASI PADA MALWARE INFORMATION SHARING PLATFORM (MISP)

Berdasarkan Cyberthreat Defense Report oleh cyber-edge pada tahun 2019, menyebutkan bahwa banyaknya data serangan yang perlu dianalisis menjadi permasalahan yang menempati peringkat pertama terkait hambatan yang dialami organisasi untuk meningkatkan efektivitas cyber-defense. Permasalahan ini juga terjadi pada implementasi *Honeypot*, banyaknya data yang dihasilkan dan tidak teridentifikasi menyebabkan implementasi *honeypot* menjadi kurang efektif. Malware Information Sharing Platform (MISP) merupakan sebuah wadah bagi *malware researcher* untuk berbagi informasi terkait insiden pada *cyber security*, penelitian ini mengusulkan metode penilaian *Indicator of Compromise* (IoC) yang berasal dari *Honeypot* berdasarkan korelasi data antara *honeypot* dan MISP. MISP dimanfaatkan sebagai *external feeder* yang digunakan untuk men-*supply* data analisis dari organisasi yang terdaftar pada MISP. *Profiling* dilakukan untuk memberikan IoC sebuah *numerical value* (0-100) yang dapat merepresentasikan tingkat bahayanya. Sistem *profiling* yang dibangun menggunakan bahasa pemrograman python dan elastic stack *Framework* pada penelitian ini berhasil membuat sistem yang dapat mengumpulkan, menyimpan, memvisualisasikan, dan melakukan penilaian terhadap IoC. Berdasarkan pengujian pada 20.471 data *honeypot*, *profile*r berhasil mengidentifikasi 3.7% serangan pada *service* smb, 82.5% serangan pada *service* mssql, 86.4% serangan pada *service* sip, 61.1% serangan pada *service* mysql, dan 87.5% serangan pada *service* mqtt.

Kata kunci: *Honeypot*, Analisis *Log*, *Threat Intelligence, Threat Intelligence Platform,* MISP, *Profiling*, Selenium, Pandas.

ABSTRACT

DESIGN OF HONEYPOT INDICATOR OF COMPROMISE (IOC) PROFILING SYSTEM BASED ON CORELATION IN MALWARE INFORMATION SHARING PLATFORM (MISP)

Based on cyber-edge Cyberthreat Defense Report in 2019, mentioning that the amount of attack data that needs to be analyzed becomes the first problem related to the obstacles experienced by organizations to improve the effectiveness of cyber-defense. This problem also occurs in honeypot implementation, the amount of data produced and unidentified causes honeypot implementation to be less effective. Malware Information Sharing Platform (MISP) is a forum for malware researchers to share information related to incidents on cyber security, this study proposes indicator of compromise (IoC) assessment method derived from Honeypot based on data correlation between honeypot and MISP. MISP is used as an external feeder used to supply analytics data from misp-listed organizations. Profiling is done to give the IOC a numerical value (0-100) that can represent the level of danger. Profiling systems built using python programming languages and elastic stack Frameworks in this study successfully created a system that can collect, store, visualize, and assess the IOC. Based on tests on 20,471 honeypot data, profilers managed to identify 3.7% of attacks on smb services, 82.5% of attacks on mssql services, 86.4% of attacks on service sips, 61.1% of attacks on mysql services, and 87.5% of attacks on mqtt services.

Keywords: Honeypot, Log Analysis, Threat Intelligence, Threat Intelligence Platform, MISP, Profiling, Selenium, Pandas.