IMPLEMENTASI SISTEM PEMANTAUN KEAMANAN JARINGAN MENGGUNAKAN HONEYPOT DAN ELK STACK (ELASTICSEARCH, LOGSTASH, KIBANA) UNTUK DETEKSI ANCAMAN SIBER DI UNJAYA

Tegar Fatwa Nugroho, Chanief Budi Setiawan

INTISARI

Latar Belakang: Dalam beberapa tahun terakhir, serangan siber meningkat signifikan, terutama pada kuartal ketiga 2024, di mana sektor pendidikan menjadi target utama. Rata-rata 3.828 serangan per minggu tercatat pada sektor ini (Check Point Research), didukung oleh data BSSN yang mencatat lonjakan anomali trafik lebih dari 330 juta selama tahun 2024. Di Indonesia, kasus kebocoran data di beberapa universitas menunjukkan pentingnya perlindungan data di lingkungan pendidikan tinggi. Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA) juga menghadapi risiko serupa akibat keterbatasan visibilitas terhadap ancaman siber.

Tujuan: Penelitian ini bertujuan mengimplementasikan sistem pemantauan keamanan jaringan di UNJAYA menggunakan honeypot OpenCanary yang terintegrasi dengan ELK Stack (Elasticsearch, Logstash, Kibana) untuk mendeteksi serangan secara real-time dan menyajikan data dalam bentuk dashboard.

Metode Penelitian: Metode penelitian yang digunakan dalam penelitian ini adalah NDLC (*Network Development Life Cycle*). Metode ini dipilih didasarkan pada kesesuaiannya dalam pengembangan sistem berbasis jaringan, khususnya dalam membangun dan mengimplementasikan sistem pemantauan keamanan jaringan.

Hasil: hasil pengujian menunjukkan bahwa sistem berhasil mendeteksi aktivitas serangan secara *real-time*, mencatat lebih dari *dua juta log* selama 30 hari monitoring, dan menampilkan data dalam *dashboard* yang informatif melalui integrasi antara OpenCanary dan ELK Stack.

Kesimpulan: Penelitian ini berhasil mengimplementasikan sistem pemantauan keamanan jaringan yang mampu mendeteksi, mencatat, dan memvisualisasikan serangan secara efektif, serta memberikan gambaran pola ancaman yang relevan untuk penguatan keamanan siber di lingkungan UNJAYA.

Kata-kunci: Keamanan Jaringan, Honeypot, OpenCanary, ELK Stack, Monitoring Jaringan

IMPLEMENTATION OF A NETWORK SECURITY MONITORING SYSTEM USING* HONEYPOT *AND ELK STACK (*ELASTICSEARCH, LOGSTASH, KIBANA*) FOR CYBER THREAT DETECTION AT UNJAYA

Tegar Fatwa Nugroho, Chanief Budi Setiawan

ABSTRACT

***Background**: in recent years, cyberattacks have significantly increased, particularly in the third quarter of 2024, with the education sector becoming a primary target. An average of 3,828 weekly attacks was recorded in this sector (Check Point Research), supported by BSSN data showing over 330 million traffic anomalies throughout 2024. In Indonesia, several data breach incidents at universities highlight the urgent need for data protection in higher education environments. Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA) faces similar risks due to limited visibility into cyber threats.*

***Objective**: This study aims to implement a network security monitoring system at UNJAYA using the OpenCanary honeypot integrated with the ELK Stack (Elasticsearch, Logstash, Kibana) to detect attacks in real time and present the data through a visual dashboard.*

***Method**: The research employs the NDLC (Network Development Life Cycle) method, chosen for its suitability in developing network-based systems, particularly for building and implementing security monitoring tools.*

***Result**: The testing results showed that the system successfully detected attack activities in real-time, recorded over two million logs during a 30-day monitoring period, and presented the data through an informative dashboard integrated with OpenCanary and the ELK Stack.*

***Conclusion**: This study successfully implemented a network security monitoring system capable of effectively detecting, logging, and visualizing cyberattacks. The system also provides insights into threat patterns that are valuable for strengthening cybersecurity at UNJAYA.*

***Keywords**: Network Security, Honeypot, OpenCanary, ELK Stack, Network Monitoring*