ANALISIS LOG MIKROTIK UNTUK MENDETEKSI SERANGAN DAN TRAFIK ANOMALI DI JARINGAN LABORATORIUM JARINGAN PRODI TEKNOLOGI INFORMASI

Khoerul Anam, Arief Ikhwan Wicaksono, Chanief Budi Setiawan

INTISARI

Latar Belakang: Analisis log MikroTik merupakan bagian penting dari strategi keamanan jaringan, dengan fokus pada deteksi dan mitigasi serangan pola trafik yang mencurigakan. Untuk mengatasi masalah ini, diperlukan melakukan penerapan kebijakan akses yang jelas dan penggunaan alat anonimisasi data untuk memberikan akses yang memadai kepada pihak-pihak yang membutuhkan informasi log untuk analisis, tanpa mengorbankan aspek keamanan jaringan.

Tujuan: Penelitian ini melakukan analisis log jaringan yang dihasilkan oleh perangkat MikroTik guna untuk mendeteksi pola trafik atau anomali yang mencurigakan pada jaringan Laboratorium Prodi Teknologi Informasi.

Metode Penelitian: Penelitian ini berfokus pada pendeteksian anomali dari log yang diperoleh dengan cara *port mirroring* dari Splunk ke mikrotik. Dalam upaya untuk memahami dan menganalisis serangan *flooding* pada jaringan

Hasil: Penelitian ini berhasil mengidentifikasi berbagai serangan, termasuk DNS Flood, SMB Flood, Telnet Flood, SSH Flood, dan serangan Metasploit. Aturan firewall di MikroTik efektif menangkap aktivitas mencurigakan. Analisis log menunjukkan pola serangan konsisten dengan puncak aktivitas pada menit ke-40 setiap jam, di mana terdeteksi 538 event.

Kesimpulan: Penelitian ini berfokus pada kapabilitas dan kapasitas MikroTik sebagai node yang mengirimkan data log ke pihak ketiga yaitu Splunk dalam upaya mendeteksi dan mengelola serangan pola trafik yang mencurigakan. Dengan menggunakan perangkat MikroTik Router dan alat analisis log seperti Splunk, penelitian ini berhasil mengidentifikasi berbagai serangan, termasuk DNS *Flood*, SMB *Flood*, Telnet Flood, SSH F*lood*, dan serangan Metasploit. Penerapan aturan firewall di MikroTik terbukti efektif dalam menangkap dan mencatat aktivitas mencurigakan. Hasil analisis log menunjukkan pola serangan yang konsisten pada waktu tertentu, dengan puncak aktivitas pada menit ke-40 dalam setiap jam. Pada menit tersebut, terdeteksi 538 *event* (97.996%), jauh lebih banyak dibandingkan menit lainnya, menunjukkan adanya aktivitas tidak biasa atau serangan yang terfokus pada waktu tersebut.

Kata-kunci: *Anomay, Flooding, Ddos, Mikrotik, Firewall,* Splunk

ANALYSIS OF MIKROTIK LOGS FOR DETECTING ATTACKS AND TRAFFIC ANOMALIES IN THE NETWORK LABORATORY OF THE INFORMATION TECHNOLOGY DEPARTMENT

Khoerul Anam, Arief Ikhwan Wicaksono, Chanief Budi Setiawan

ABSTRACK

***Background**: Analyzing MikroTik logs is a crucial part of network security strategies, focusing on detecting and mitigating suspicious traffic patterns. To address this issue, it is necessary to implement clear access policies and use data anonymization tools to provide adequate access to those who need log information for analysis without compromising network security.*

***Objective**: This study aims to analyze network logs generated by MikroTik devices to detect suspicious traffic patterns or anomalies in the Information Technology Laboratory network.*

***Research Method**: This study focuses on anomaly detection from logs obtained through port mirroring from Splunk to MikroTik. The goal is to understand and analyze flooding attacks on the network.*

***Results**: The study successfully identified various attacks, including DNS Flood, SMB Flood, Telnet Flood, SSH Flood, and Metasploit attacks. Firewall rules on MikroTik effectively captured suspicious activities. Log analysis showed consistent attack patterns with peak activity at the 40th minute of each hour, where 538 events were detected.*

***Conclusion**: This study focuses on the capability and capacity of MikroTik as a node that sends log data to a third party, Splunk, in an effort to detect and manage suspicious traffic patterns. Using MikroTik Routers and log analysis tools like Splunk, this study successfully identified various attacks, including DNS Flood, SMB Flood, Telnet Flood, SSH Flood, and Metasploit attacks. The application of firewall rules on MikroTik proved effective in capturing and logging suspicious activities. The log analysis results showed consistent attack patterns at specific times, with peak activity at the 40th minute of each hour. At that minute, 538 events (97.996%) were detected, significantly more than other minutes, indicating unusual activity or focused attacks at that time.*

***Keywords**: Anomaly, Flooding, DDoS, MikroTik, Firewall, Splunk*