EVALUASI ANOMALI DALAM LALU LINTAS JARINGAN UNJAYA UNTUK MENGIDENTIFIKASI POTENSI ANCAMAN KEAMANAN

Susi Dwi Nur Putri, Arief Ikhwan Wicaksono, Chanief Budi Setiawan

INTISARI

Latar Belakang: Jaringan komputer memainkan peran vital dalam berbagai sektor, termasuk pendidikan, dengan mendukung sistem *e-learning* dan layanan administratif di institusi seperti Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA). Meskipun manfaatnya besar, risiko keamanan juga meningkat, termasuk ancaman siber yang dapat merusak data dan operasi. Anomali dalam trafik jaringan menjadi indikasi potensial serangan siber atau kegagalan sistem. Untuk melindungi integritas dan kerahasiaan data, analisis trafik jaringan menggunakan teknik *Port Mirroring* dan file PCAP adalah metode yang krusial. DynamiteLab, sebagai alat analisis trafik jaringan, menawarkan kemampuan mendalam untuk mendeteksi pola mencurigakan dan potensi ancaman.

Tujuan: Penelitian ini bertujuan mengevaluasi efektivitas DynamiteLab dalam menganalisis data PCAP untuk mendeteksi aktivitas trafik mencurigakan di jaringan Kampus 1 UNJAYA dan meningkatkan keamanan sistem informasi.

Metode Penelitian: Penelitian ini menggunakan teknik *Port Mirroring* untuk mengumpulkan data trafik jaringan di Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA). Data yang diperoleh disimpan dalam format PCAP, yang kemudian dianalisis menggunakan perangkat lunak DynamiteLab.

Hasil: Penelitian ini menggunakan DynamiteLab untuk menganalisis file PCAP dari jaringan Kampus 1 UNJAYA, menemukan pola anomali trafik, IP mencurigakan, dan potensi malware. Temuan utama meliputi dominasi peringatan pada protokol TCP dan UDP serta aktivitas terkait jaringan P2P dan Tor. Penelitian ini menyoroti perlunya pengawasan tambahan dan evaluasi keamanan untuk menangani ancaman yang terdeteksi.

Kesimpulan: Penelitian ini menemukan bahwa analisis trafik jaringan di Kampus 1 UNJAYA dengan DynamiteLab mengidentifikasi aktivitas mencurigakan, terutama terkait protokol TCP dan UDP. TCP menyumbang 66% dan UDP 44% dengan peringatan utama berupa Misc Attack dan Potential Corporate Privacy Violation. Host internal dan eksternal menjadi titik perhatian utama, terutama host internal.

Kata-kunci: *Traffic Analysis*, *Packet Capture (PCAP)*, *Anomaly Detection*, DynamiteLab

EVALUATION OF ANOMALIES IN NETWORK TRAFFIC UNJAYA TO IDENTIFY POTENTIAL SECURITY THREATS

Susi Dwi Nur Putri, Arief Ikhwan Wicaksono, Chanief Budi Setiawan

ABSTRACT

***Background**: Computer networks play a vital role in various sectors, including education, by supporting e-learning systems and administrative services at institutions such as Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA). While the benefits are great, security risks are also increasing, including cyber threats that can damage data and operations. Anomalies in network traffic are indicative of potential cyberattacks or system failures. To protect data integrity and confidentiality, analyzing network traffic using Port Mirroring techniques and PCAP files is a crucial method. DynamiteLab, as a network traffic analysis tool, offers in-depth capabilities to detect suspicious patterns and potential threats.*

***Objective**: This study aims to evaluate the effectiveness of DynamiteLab in analyzing PCAP data to detect suspicious traffic activity on the UNJAYA Campus 1 network and improve information system security.*

***Method**: This study uses Port Mirroring technique to collect network traffic data at Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA). The data obtained is stored in PCAP format, which is then analyzed using DynamiteLab software.*

***Result**: This study used DynamiteLab to analyze PCAP files from UNJAYA's Campus 1 network, finding anomalous traffic patterns, suspicious IPs, and potential malware. Key findings included a predominance of alerts on TCP and UDP protocols as well as activity related to P2P and Tor networks. This research highlights the need for additional surveillance and security evaluation to address the detected threats.*

***Conclusion**: This study found that analyzing network traffic at UNJAYA Campus 1 with DynamiteLab identified suspicious activity, mainly related to TCP and UDP protocols. TCP accounted for 66% and UDP 44% with the main warnings being Misc Attack and Potential Corporate Privacy Violation. Internal and external hosts are the main points of concern, especially internal hosts.*

***Keywords**: Traffic Analysis, Packet Capture (PCAP), Anomaly Detection,* DynamiteLab