BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Jaringan komputer menjadi sangat penting dalam era digital yang semakin maju, dan sangat penting untuk berbagai operasi, termasuk bisnis, pendidikan, pemerintahan, dan kehidupan sehari-hari (Saputra et al., 2023). Saat ini, institusi pendidikan seperti Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA) sangat bergantung pada teknologi jaringan untuk mendukung berbagai bagian operasi mereka, seperti sistem *e-learning*, manajemen administrasi, dan layanan akademik lainnya. Sistem jaringan yang canggih ini memungkinkan mahasiswa, dosen, dan karyawan mengakses sumber daya pendidikan dengan lebih efisien dan fleksibel, tanpa terbatas ruang atau waktu.

Namun, meskipun teknologi ini memiliki manfaat, penggunaan ini juga membawa risiko keamanan yang signifikan. Berbagai jenis serangan siber dapat terjadi pada institusi pendidikan seperti UNJAYA. Ini termasuk serangan yang dimaksudkan untuk mencuri data sensitif, mengganggu layanan, atau merusak reputasi lembaga. Adanya anomali atau kelainan dalam trafik jaringan, yang dapat menunjukkan serangan siber atau kegagalan sistem, merupakan salah satu ancaman yang paling signifikan (Najib et al., 2020). Keamanan sistem informasi sangat penting untuk menjaga data mahasiswa aman, menjaga kerahasiaan data pribadi, dan memastikan bahwa kampus beroperasi dengan lancar.

Bagian Siber dan Sandi Negara (BSSN) melaporkan bahwa sebanyak 74 juta anomali trafik terdeteksi pada awal tahun 2024. Sekitar 59,76% atau 44.637.929 dari anomali tersebut diidentifikasi sebagai aktivitas malware. Peningkatan ini menunjukkan peningkatan besar dalam serangan siber, setelah BSSN mencatat 1,6 miliar serangan siber pada tahun 2021, yang didominasi oleh aktivitas malware dan Trojan. BSSN secara aktif memantau dan menganalisis aktivitas malware (CNN Indonesia, 2024).

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

Keamanan sistem jaringan komputer dapat didefinisikan sebagai upaya untuk melindungi data dan sumber daya dari orang yang tidak berhak mengaksesnya, perusakan, dan penggunaan yang tidak sah (Hardani & Ramli, 2022). Bagaimana mendeteksi dan merespons dengan cepat terhadap pola aktivitas mencurigakan merupakan salah satu tantangan utama yang dihadapi. Ini mencakup menemukan serangan yang sedang berlangsung dan membuat rencana untuk mencegah serangan sebelum menyebabkan kerusakan besar. Dalam situasi seperti ini, analisis trafik jaringan merupakan komponen penting dalam meningkatkan kemampuan organisasi untuk menangani ancaman siber.

PCAP *(Packet Capture)* adalah format file yang menyimpan data paket jaringan yang dikumpulkan dari antarmuka jaringan dan sering digunakan untuk analisis dan pemecahan masalah jaringan. File PCAP berisi data mentah dari paket jaringan, termasuk header dan payload setiap paket. File ini dapat dihasilkan oleh alat penangkap paket seperti Wireshark, tcpdump, atau perangkat lunak pemantauan jaringan lainnya. PCAP sangat berguna dalam analisis dan keamanan jaringan, memungkinkan administrator jaringan atau analisis untuk memeriksa dan menganalisis lalu lintas jaringan untuk berbagai tujuan (Keary, 2023).

Penelitian ini memfokuskan pada pemanfaatan file PCAP untuk menganalisis trafik jaringan di Kampus 1 Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA) dengan bantuan alat DynamiteLab, sebuah platform yang dikenal karena kemampuannya dalam analisis trafik jaringan yang mendalam dan real-time. Proses ini melibatkan teknik *Port Mirroring* untuk menangkap semua lalu lintas yang melalui switch jaringan dan menyimpannya dalam format PCAP. Data yang disimpan dalam format PCAP akan dianalisis untuk mendeteksi dan menganalisis pola lalu lintas jaringan yang mencurigakan, membantu dalam mengidentifikasi potensi ancaman keamanan.

Penerapan metode ini diharapkan dapat mengarah pada peningkatan keamanan sistem informasi di UNJAYA, pengurangan risiko serangan siber, dan penguatan perlindungan terhadap ancaman yang ada. Keuntungan dari metode ini tidak hanya akan meningkatkan keamanan data dan operasional, tetapi juga memperkuat kepercayaan pihak berwenang terhadap manajemen informasi

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

akademik. Dengan demikian, penggunaan file PCAP untuk analisis dan deteksi pola mencurigakan melalui Dynamitelab akan memainkan peran penting dalam melindungi aset digital UNJAYA dan mendukung tujuan pendidikan institusi secara keseluruhan.

1.2 PERUMUSAN MASALAH

Keamanan jaringan merupakan aspek krusial bagi institusi pendidikan seperti Kampus 1 UNJAYA, terutama dalam menghadapi ancaman siber yang semakin rumit. Seiring dengan kemajuan teknologi, terdapat kebutuhan yang meningkat untuk metode yang efisien dalam mendeteksi dan menganalisis lalu lintas jaringan. Implementasi *Port Mirroring* yang efektif untuk memperoleh data yang akurat dan representatif menjadi salah satu tantangan. Selain itu, perlu dilakukan analisis untuk mengidentifikasi pola trafik mencurigakan dari data yang dikumpulkan. Oleh karena itu, penting untuk mengevaluasi efektivitas dan akurasi DynamiteLab sebagai alat analisis dalam mendeteksi ancaman di jaringan Kampus 1 UNJAYA.

1.3 BATASAN MASALAH

Penelitian ini hanya mencakup analisis data lalu lintas jaringan dari Kampus 1 UNJAYA, dengan penekanan pada deteksi dan analisis pola trafik mencurigakan. Penelitian ini tidak mencakup penanganan atau perbaikan langsung terhadap ancaman yang teridentifikasi.

1.4 PERTANYAAN PENELITIAN

Berdasarkan perumusan masalah di atas, pertanyaan penelitian yang akan dijawab dalam penelitian ini adalah:

1. Seberapa efektif Dynamitelab dalam mengidentifikasi trafik jaringan yang mencurigakan?
2. Apa jenis anomali trafik yang dapat dideteksi oleh DynamiteLab pada jaringan Kampus 1 UNJAYA?
3. Apa hasil utama dari analisis trafik jaringan di Kampus 1 UNJAYA yang dilakukan menggunakan Dynamitelab?

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

1.5 TUJUAN PENELITIAN

Penelitian ini bertujuan untuk menggunakan DynamiteLab dalam menganalisis data PCAP yang diperoleh melalui teknik *Port Mirroring*, dengan tujuan utama mendeteksi dan mengidentifikasi aktivitas trafik mencurigakan di jaringan Kampus 1 UNJAYA.

1.6 MANFAAT HASIL PENELITIAN

Penelitian ini diharapkan dapat memberikan manfaat yang berarti bagi berbagai pihak yang terlibat, di antaranya:

1. Memperluas pemahaman tentang teknik pengumpulan dan analisis trafik jaringan dengan menggunakan alat seperti Dynamitelab.
2. Menyediakan informasi yang dapat dimanfaatkan untuk meningkatkan keamanan jaringan di Kampus 1 UNJAYA.
3. Menambah referensi terkait penggunaan alat analisis trafik jaringan untuk mendeteksi ancaman keamanan, serta memberikan panduan praktis dalam penerapannya di lingkungan kampus atau institusi lainnya.

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA