BAB 1

PENDAHULUAN

1.1. Latar Belakang

Dalam lingkungan akademik, ketersediaan dan keamanan jaringan sangat penting untuk menjamin kelancaran pelayanan dan proses belajar-mengajar. Serangan jaringan seperti *malware*, virus, dan *Denial of Service* (DoS) dapat membahayakan sistem dan data yang tersimpan pada *server*. Serangan jaringan juga semakin beragam dan berbahaya. Serangan jaringan saat ini dapat dilakukan oleh siapa saja, baik individu atau kelompok yang tidak bertanggung jawab. Oleh karena itu, *server* dan jaringan komputer harus dilindungi dari serangan yang dapat menyebabkan kerusakan dan kehilangan data.

Server merupakan komponen kunci dari insfrastruktur jaringan yang ada pada Universitas Muhammadiyah Kalimantan Timur (UMKT). *Server* menyediakan layanan untuk jaringan, seperti penyimpanan data, pemprosesan data, dan aplikasi. Ada banyak ancaman yang dapat menyerang *server*, baik saat berada dalam pengawasan administrator maupun tidak. Oleh karena itu, diperlukan sistem keamanan untuk mendeteksi dan mencegah serangan secara *real-time* terlepas dari *server* itu berada dalam pengawasan maupun tidak agar dapat mengurangi dampak yang ditimbulkan oleh serangan jaringan tersebut. Salah satu cara untuk melindungi jaringan komputer adalah dengan menerapkan *Instrusion Detection System* (IDS).

Suricata merupakan IDS *open source* dengan kemampuan mendeteksi serangan pada jaringan menggunakan konfigurasi *rules* yang tepat (Syani, 2020). Suricata mampu melakukan analisis lalu lintas jaringan komputer secara *real-time*, memantau lalu lintas jaringan komputer menggunakan IDS, mencegah instrusi *online*, dan melakukan proses *packet capture* (pcap) *offline*. Dengan kemampuan tersebut Suricata dapat dijadikan sebagai *next generation* IDS. Maka, pada penelitian ini akan menerapkan atau mengimplementasikan IDS Suricata pada jaringan komputer Universitas Muhammadiyah Kalimantan Timur (UMKT). IDS Suricata dipilih karena mampu mendeteksi ancaman serangan pada jaringan

secara *real-time* dan memiliki kemampuan untuk melakukan analisis lebih akurat dari IDS lainnya.

Berdasarkan uraian diatas, maka penulis akan melakukan penelitian dengan judul "Pendeteksi dan Pencegahan Serangan Jaringan Menggunakan *Instrusion Detection System* (IDS) Suricata studi kasus Universitas Muhammadiyah Kalimantan Timur". Melalui penelitian ini diharapkan sistem keamanan jaringan pada UMKT dapat ditingkatkan, ancaman serangan dapat dideteksi lebih awal, dan langkah-langkah pencegahan dapat dilakukan dengan cepat untuk mengurangi dampak dari serangan. Penelitian ini juga diharapkan dapat menjadi referensi bagi pengembangan sistem keamanan jaringan yang lebih baik.

1.2. Rumusan Masalah

Banyak ancaman yang dapat menyerang *server* jaringan komputer, baik saat berada dalam pengawasan administrator maupun tidak. Untuk mengatasi hal tersebut, dibutuhkan *Instrusion Detection System* (IDS) yang mampu mendeteksi dan mencegah serangan secara *real-time* agar mengurangi dampak yang ditimbulkan.

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan diatas, tujuan yang ingin dicapai dari penelitian ini adalah menerapkan sistem *Instrusion Detection System* (IDS) menggunakan prangkat lunak *open source* Suricata untuk mendeteksi dan mencegah ancaman serangan pada *server* jaringan komputer UMKT. IDS Suricata dipilih karena dapat melakukan deteksi ancaman serangan secara *real-time* dan memiliki kemampuan untuk melakukan analisis yang lebih akurat dari IDS lainnya.

1.4. Batasan Masalah

Untuk menghindari penyimpangan dari judul dan tujuan yang sebenarnya maka dibuatkan ruang lingkup Batasan masalah sebagai berikut:

1. Penelitian ini difokuskan untuk meneliti keamanan jaringan pada *server* jaringan komputer yang terdapat di Universitas Muhammadiyah Kalimantan Timur (UMKT)

2. Sistem Pendeteksi dan Pencegahan serangan jaringan yang digunakan hanya menggunakan *Instrusion Detection System* (IDS) Suricata sebagai solusi keamanan dari peneliti.
3. Penelitian tidak mencakup aspek lain dari keamanan jaringan seperti penggunaan enkripsi atau autentikasi.
4. Penelitian ini hanya melakukan uji coba pada jaringan *server* Universitas Muhammadiyah Kalimantan Timur (UMKT) dan tidak diuji pada jaringan lain.