BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam beberapa tahun terakhir, serangan siber meningkat pesat terutama pada kuartal ketiga tahun 2024. Laporan *Check Point Research* mencatat rata-rata serangan mingguan per organisasi mencapai 1.876. Serangan tersebut mengalami kenaikan 75% dibandingkan periode yang sama pada 2023 dan 15% dari kuartal sebelumnya. Sektor pendidikan dan penelitian menjadi target utama dengan 3.828 serangan per minggu, diikuti oleh sektor pemerintah/militer 2.553 serangan dan kesehatan 2.434 serangan. Lonjakan ini menunjukkan meningkatnya ancaman terhadap keamanan data, terutama pada sektor yang mengelola informasi sensitif. Laporan *Check Point Research* semakin diperkuat oleh data dari Badan Siber dan Sandi Negara (BSSN) dalam lanskap keamanan siber 2024. BSSN mencatat 330.527.636 anomali trafik sepanjang tahun 2024, dengan lonjakan tertinggi pada bulan Desember mencapai 112.085.045 anomali, sementara jumlah terendah terjadi pada bulan Mei dengan 12.273.078 anomali (BSSN, 2024).

Studi yang dilakukan oleh (Lallie dkk., 2023) semakin menguatkan bahwa sektor pendidikan menjadi target utama serangan siber. Penelitian ini mencatat setidaknya 58 serangan yang teridentifikasi menyerang universitas, termasuk kasus *ransomware* yang memaksa *Maastricht University* membayar 200.000 USD dan *University of California*, San Francisco membayar 1,14 juta USD untuk memulihkan data yang diretas. Di Indonesia, dugaan serangan siber pada tahun 2024 menimpa Universitas Indonesia (UI), dimana lebih dari 10.000 data pengguna diduga bocor dan diperjualbelikan di forum gelap yang memicu kekhawatiran terkait perlindungan data di Institusi Pendidikan.

Meningkatnya tren serangan siber yang menargetkan sektor pendidikan dan penelitian terutama universitas, menuntut institusi pendidikan di Indonesia untuk lebih waspada. Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA) tidak terkecuali dari risiko ini, terutama karena ketergantungannya pada sistem berbasis

teknologi informasi dalam operasional akademik dan administrasi. Dengan layanan berbasis *website* dan portal akademik, UNJAYA menyimpan data penting, termasuk informasi akademik, penelitian, serta data pribadi mahasiswa dan staf, yang rentan terhadap ancaman siber.

Salah satu tantangan utama dalam menghadapi serangan siber adalah keterbatasan visibilitas terhadap ancaman yang mengintai. Tanpa sistem pemantauan yang efektif banyak serangan yang terjadi tanpa terdeteksi hingga dapat menimbulkan dampak yang signifikan. Ketidakmampuan dalam mendeteksi pola serangan sejak dini membuat respon terhadap ancaman menjadi rektif dan kurang optimal. Oleh karena itu diperlukan solusi yang mampu meningkatkan visibilitas keamanan siber dengan mendeteksi, menganalisis, dan memvisualisasikan ancaman secara *real-time.*

Mengingat tingginya frekuensi serangan, strategi mitigasi yang diterapkan harus bersifat proaktif dan mampu mendeteksi potensi ancaman sebelum terjadi insiden yang lebih besar. Maka dari itu UNJAYA perlu menerapkan Langkah strategis untuk meningkatkan keamanan siber di lingkungan kampus.

1.2 Perumusan Masalah

Rumusan Masalah penelitian ini berdasarkan pada fakta bahwa Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA) saat ini belum memiliki sistem pemantauan keamanan yang mampu mendeteksi dan memberikan peringatan dini terhadap serangan siber secara *real-time.*

1.3 Pertanyaan Penelitian

Berdasarkan latar belakang yang telah dijelaskan, dapat ditarik beberapa pertanyaan penelitian antara lain:

1. Bagaimana proses implementasi sistem pemantauan keamanan jaringan menggunakan honeypot dan ELK *Stack* (Elasticsearch, Logstash, Kibana) di Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA)?

2. Informasi apa saja yang disajikan pada *dashboard* sistem pemantauan keamanan jaringan, dan bagaimana visualisasi data tersebut dapat membantu dalam analisis keamanan jaringan di UNJAYA?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah mengimplementasikan sistem pemantauan keamanan jaringan di UNJAYA menggunakan honeypot untuk mendeteksi serangan secara *real-time*, serta mengintegrasikan honeypot dengan ELK *stack (*Elasticsearch, Logstash, Kibana*)* sehingga *log* serangan yang terkumpul dapat diolah dan divisualisasikan dalam bentuk *dashboard* yang informatif.

1.5 Manfaat Hasil Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik dalam ranah akademik maupun praktis, khususnya dalam bidang keamanan jaringan. Manfaat yang diperoleh antara lain:

1. Membantu UNJAYA dalam membangun sistem pemantauan keamanan jaringan yang mampu mendeteksi serangan siber secara *real-time* dan menganalisis pola serangan melalui visualisasi *log* di ELK *Stack*.
2. Integrasi honeypot dan ELK Stack akan meningkatkan efektivitas dalam mendeteksi dan merespon serangan siber sehingga mitigasi ancaman dapat dilakukan dengan cepat dan akurat.

1.6 Batasan Penelitian

Agar penelitian ini memiliki fokus yang jelas dan terarah, maka ruang lingkup pembahasan dibatasi pada aspek-aspek teknis yang mendukung implementasi dan pengujian sistem pemantauan keamanan jaringan menggunakan honeypot dan ELK Stack di lingkungan Universitas Jenderal Achmad Yani Yogyakarta (UNJAYA). Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Pembangunan dan implementasi sistem pemantaun keamanan jaringan berbasis honeypot OpenCanary yang dikonfigurasi untuk mensimulasikan

layanan FTP, HTTP, SSH, SMTP, Telnet, MySQL, SMB, RDP, MSSQL, Git.

2. Sistem pemantauan dikembangkan pada lingkungan jaringan laboratorium dan jaringan publik UNJAYA, namun tidak mencakup integrasi langsung dengan sistem jaringan utama atau perangkat keamanan lain seperti *firewall* dan IDS/IPS.
3. Pengolahan dan visualisasi data log dilakukan menggunakan komponen ELK Stack (Elasticsearch, Logstash, dan Kibana), dengan data *log* yang ditangkap oleh honeypot dikirim melalui Filebeat untuk selanjutnya diproses dan divisualisasikan dalam bentuk *dashboard*.
4. Penelitian ini tidak mencakup pengujian terhadap efektivitas mitigasi serangan atau penerapan tindakan pencegahan, tetapi hanya berfokus pada pencatatan, pengolahan, dan penyajian *log* serangan sebagai alat bantu analisis keamanan jaringan.