BAB 1
USULAN GAGASAN

1.1 Deskripsi Umum Masalah

Ancaman terhadap keamanan siber semakin kompleks, diiring dengan berkembangnya berbagai teknik dan alat serangan. Salah satu bentuk ancaman yang signifikan adalah *malware*, seperti *worm*, *rootkit,* dan *exploit tools*, yang sering digunakan dalam serangan kategori *Remote to Local* dan *User to Root*. Selain itu, terdapat pula jenis serangan lain seperti *Denial of Service* (DoS) dan *Probe*, yang meskipun tidak selalu melibatkan *malware*, tetap menjadi bagian penting dalam lanskap ancaman siber karena dapat mengganggu layanan dan melakukan pemetaan sistem target.

Berdasarkan laporan *Verizon Data Breach Investigations Report* (2024), sekitar 14% insiden keamanan terjadi akibat eksploitasi atau serangan terhadap kerentanan perangkat, menunjukkan peningkatan signifikan dibandingkan tahun sebelumnya [1]. Di Indonesia, Laporan Tahunan Badan Siber dan Sandi Negara (2023) mencatat lebih dari 404 juta trafik anomali serangan, mencerminkan tingginya intensitas ancaman siber di tingkat nasional [2]. Data ini menunjukkan bahwa baik secara global maupun nasional, ancaman siber terus berkembang dan semakin beragam.

Meskipun serangan berbasis *malware* menjadi salah satu ancaman utama secara global, serangan *Distributed Denial of Service* juga tercatat sebagai salah satu jenis serangan yang paling sering terjadi di Indonesia. Namun, dalam penelitian ini digunakan pendekatan berbasis DoS sebagaimana diklasifikasikan dalam dataset NSL-KDD, karena lebih sesuai untuk kebutuhan simulasi dan pengujian sistem deteksi intrusi dalam sistem terbatas.

Oleh karena itu, pengembangan sistem deteksi terhadap berbagai jenis serangan, termasuk DoS, Probe, R2L, dan U2R, menjadi langkah penting dalam memperkuat keamanan jaringan. Hal ini menunjukkan perlunya perhatian lebih dalam mempertahankan serta mengamankan sistem jaringan, terutama dalam melindungi data yang bersifat vital. Salah satu keterbatasan sistem keamanan konvensional adalah penggunaan *Intrusion Prevention System* berbasis aturan statis, yang sering kali tidak mampu mendeteksi serangan dengan pola yang tidak dikenal atau bersifat dinamis. Sistem seperti ini sangat bergantung pada pendekatan *signature-based*, sehingga kurang efektif dalam menghadapi serangan yang kompleks dan terus berkembang.

Intrusion Prevention System merupakan salah satu pendekatan sistem keamanan jaringan dengan tujuan untuk membangun sistem keamanan komputer, dimana IPS menggunakan metode kombinasi yang secara teknis ada pada *firewall* dan metode *Intrusion Detection System* dengan sangat sistematis [3]. IPS memiliki kemampuan untuk inspeksi terhadap aliran trafik paket data dalam jaringan dan memeriksa paket tersebut apakah paket yang melewati jaringan sesuai dengan daftar aturan-aturan yang telah dikonfigurasi pada sistem atau tidak. Namun, jika ada serangan yang tidak sesuai dengan aturan yang ada pada sistem, IPS cenderung mengabaikannya dan menganggap paket tersebut sebagai paket yang tidak berbahaya dan diteruskan berdasarkan alamat tujuannya. Hal ini menjadi kelemahan yang serius ketika berhadapan dengan serangan yang tidak dikenal atau pola serangan baru yang belum tercakup oleh aturan statis tersebut.

Salah satu tantangan utama dalam penerapan sistem deteksi serangan secara *real-time* adalah menjaga agar proses identifikasi tetap berlangsung cepat dan akurat tanpa mengorbankan kinerja sistem. Penggunaan algoritma machine learning yang kompleks, terutama ketika seluruh fitur digunakan seperti pada dataset NSL-KDD, dapat meningkatkan akurasi, namun juga menimbulkan tantangan dalam hal efisiensi pemrosesan dan kebutuhan pelatihan ulang model [4]. Oleh karena itu, penting untuk mempertimbangkan strategi pemilihan fitur dan efisiensi sistem agar tetap mampu merespons secara efektif dalam kondisi trafik jaringan yang tinggi.

Penelitian ini bertujuan untuk mengembangkan sistem keamanan siber yang lebih adaptif dengan mengintegrasikan metode *machine learning* berbasis algoritma yang relevan seperti K-Means, Naive Bayes, Neural Network, dan XGBoost ke dalam *Intrusion Prevention System* (IPS). Dalam sistem ini, *core engine* IPS akan diintegrasikan dengan plugin DPX melalui komunikasi API agar mampu menerima masukan dari model *machine learning*. Pada dasarnya, *machine learning* melibatkan penggunaan algoritma dan model statistik untuk melatih sistem agar dapat mengenali pola dan membuat prediksi berdasarkan data yang diberikan [5].

Dengan pendekatan ini, IPS dapat belajar dan mengenali pola serangan baru yang tidak terdeteksi oleh aturan statis konvensional. Setelah pengujian berakhir, IPS akan menghasilkan data berupa log, dimana data log tersebut akan dikirimkan, diolah, dan divisualisasikan melalui platform Wazuh yang berfungsi sebagai *Security Information and Event Management* (SIEM).

Dengan menggunakan Wazuh, data log dari klasifikasi *machine learning* dapat diindeks, dianalisis, dan dihubungkan dengan *rule* deteksi keamanan lainnya untuk memberikan visualisasi atau gambaran yang komprehensif mengenai potensi ancaman dan aktivitas mencurigakan di suatu jaringan. Wazuh tidak hanya mengumpulkan dan menganalisis data keamanan, tetapi juga menyediakan deteksi intrusi dan kerentanan deteksi serta pemantauan terhadap aturan yang diterapkan dalam sistem [6]. Platform ini menyediakan laporan terperinci yang memudahkan pemantauan keamanan jaringan secara keseluruhan serta memberikan evaluasi terhadap sistem kemananan yang diimplementasikan. Dengan hal tersebut,secara signifikan mampu meningkatkan kemampuan deteksi dan pencegahan terhadap serangan siber yang lebih kompleks dan canggih sehingga menjadikan sistem lebih responsif serta tetap terkendali dalam menghadapi ancaman yang berkembang.

Pengujian dilakukan dengan mengukur akurasi deteksi serangan melalui beberapa parameter utama, seperti *precision* (jumlah serangan berdasarkan hasil prediksi), *recall* (jumlah serangan yang benar benar terjadi), *f1-score* (rata rata dari hasil *precision* dan *recall*), dan *accuracy*. Pengukuran ini menjadi fokus utama dalam mengevaluasi sistem untuk meningkatkan kinerja deteksi serangan berbasis *machine learning*. Selain itu, pengujian juga mencakup pengukuran waktu latih (*training*) dan waktu prediksi dari proses *machine learning* untuk menilai efisiensi waktu dalam mendeteksi ancaman.

1.2 Analisis Masalah

Masalah Serangan siber sering kali sulit dideteksi secara dini karena pola serangan yang beragam dan tidak terduga. Adapun aspek-aspek permasalahan yang akan diangkat dan dijabarkan sebagai berikut:

1.2.1 Aspek Teknologi

Serangan siber seperti Denial of Service, Probe, Remote to Local, dan User to Root dapat menyebabkan gangguan layanan, pencurian data, hingga pengambilalihan akses sistem secara tidak sah [7]. Serangan-serangan ini sering kali sulit dideteksi karena menggunakan pola yang kompleks dan dinamis. Untuk mendeteksi serangan ini secara efektif, sistem keamanan perlu dioptimalkan dengan algoritma machine learning seperti XGBoost, yang mampu memproses data secara cepat, akurat, dan efisien dalam jaringan *real-time*.

Tantangannya adalah bagaimana memilih dataset yang relevan, dan mengelola sumber daya yang terbatas tanpa menyebabkan kelebihan beban yang dapat mengakibatkan *overload* hingga crash [8]. Integrasi machine learning dengan Snort sebagai IPS dan Wazuh sebagai platform SIEM sangat penting untuk memastikan deteksi dan pencegahan serangan yang efisien dan responsif.

1.2.2 Aspek Regulasi dan Hukum

Dalam mengembangkan sistem keamanan siber, sangat penting untuk mematuhi regulasi dan hukum yang berlaku, baik di tingkat nasional maupun internasional, seperti GDPR atau General Data Protection Regulation di Eropa dan undang-undang baru yang dibentuk di Indonesia yaitu UU-PDP atau Undang-Undang Perlindungan Data Pribadi [9] serta standar keamanan siber lainnya seperti ISO/IEC 27001. Sistem keamanan harus memastikan bahwa pengumpulan, pemrosesan, dan penyimpanan data dilakukan secara transparan dan aman [10]. Selain itu, sistem juga perlu memiliki mekanisme audit yang kuat untuk membuktikan kepatuhan terhadap regulasi, terutama dalam hal pelanggaran keamanan yang dapat menyebabkan kebocoran data. Penanganan insiden keamanan harus dilakukan dengan cepat dan sesuai peraturan, seperti kewajiban pelaporan kepada Badan Siber dan Sandi Negara (BSSN) di Indonesia [11]. Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11/2008 yang mengatur perihal Aspek Ruang Digital diantaranya :

- Pasal 30: Larangan akses ilegal ke sistem elektronik milik orang lain.
- Pasal 32: Larangan mengubah, merusak, atau menghilangkan informasi elektronik milik pihak lain.
- Pasal 35: Larangan menciptakan informasi elektronik atau dokumen elektronik palsu untuk menyesatkan pihak lain.

Adapun aturan lain yang berlaku seperti aturan pada Undang-Undang No. 3 Tahun 2002 yang berfokus pada Pengaturan Pertahanan Negara:

- Pasal 7 Ayat (2): Ancaman nonmiliter, termasuk ancaman siber, diatur sebagai bagian dari komponen pertahanan negara.
- Pasal 20: Setiap warga negara wajib ikut serta dalam usaha pertahanan dan keamanan negara.

Sesuai dengan Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik (PP PSTE) yang mengatur Teknis Penyelenggaraan Sistem Elektronik Dan Transaksi Elektronik:

Pasal 17: Penyelenggara wajib melindungi data pribadi yang disimpan atau diproses dalam sistem elektronik.

Pasal tersebut mengatur tentang pengelolaan dan perlindungan data pribadi yang harus dilakukan oleh penyelenggara sistem elektronik. Hal ini mencakup kewajiban untuk menjaga kerahasiaan, integritas, dan ketersediaan data yang dikelola sehingga sistem keamanan dapat dikatakan layak memenuhi kriteria tersebut, sehingga didapatkan lah pedoman yang tidak hanya diberikan pada pengguna namun terhadap perusahaan atau penyelenggara elektronik tertentu serta penentu urgensi dari topik yang akan diambil.

Acuan perancangan ini berdasarkan standar pedoman *IEEE Guide for Developing System Requirements Specifications Std 1233-1998*, diklasifikasikan bahwa untuk merancang suatu batasan spesifikasi memiliki tiga faktor yang dianggap penting, yaitu (1) Pengguna, (2) Lingkungan, (3) Komunitas Teknis [12]. Dari sudut pandang pengguna, informasi diperoleh terhadap perihal permintaan pengguna yang menjadi landasan utama dalam pengembangan sistem. Kemudian dari sudut pandang lingkungan, batasan dan standar yang terkait dengan pembangunan sistem yang direncanakan diidentifikasi. Pada saat yang sama, dari sudut pandang komunitas teknis, terdapat akses terhadap informasi mengenai desain yang dapat digunakan dan rincian teknis.

1.2.3 Aspek Bisnis dan Sosial

Serangan siber sangat merugikan bagi perusahaan, hal ini dikarenakan penyerang dapat mengambil alih dan mendapatkan hak administratif serta dapat mempengaruhi reputasi bisnis. Penyerang dapat membuat layanan ataupun aplikasi dari target tidak dapat diakses, hal ini dapat menyebabkan turunnya kualitas SLA atau *Service Level Agreement* yang merupakan perjanjian tingkat layanan yang berisi kesepakatan antara penyedia layanan dan pelanggan. Sehingga, hal ini dapat memberikan reputasi bisnis yang buruk dan mengakibatkan kesulitan dalam akses layanan/media, penurunan produktivitas, meruginya perusahaan dan lain sebagainya [13] [14].

Kemudian dari serangan siber ini juga dapat merugikan individu atau seseorang sehingga dapat berdapat pada bidang sosial seseorang, seperti penyebaran hoax, identitas data yang bocor hingga disalahgunakan oleh pihak yang tidak bertanggung jawab. Hal tersebut tentu saja merugikan dikarenakan seseorang akan menjadi korban yang berakibatkan bullying, dikucilkan bahkan dijauhi dalam kehidupan sosial bahkan hingga masalah yang serius terjadinya tagihan atau hutang yang bukan milik orang itu sendiri [15] [16].

1.3 Analisis Solusi yang Ada

Pengamanan dan pencegahan terhadap serangan siber memberikan beberapa solusi yang digunakan pada penelitian ini. Solusi yang ditawarkan merupakan penggunaan Snort dan yang dibantu oleh Machine Learning sebagai algoritma pemrosesan serangan siber seperti Kmeans, Neural Network, Naive Bayes dan XGBoost sebagai pendeteksinya. Pada penelitian ini sebuah *server dummy* diserang sehingga serangan tersebut dideteksi sehingga memudahkan system untuk memberikan sebuah solusi dan pencegahan terhadap *breach* yang terjadi. Fitur – fitur yang digunakan pada penelitian ini adalah *IPS, ML, dan SIEM.*

1.4 Tujuan Tugas Akhir

Tujuan dari sistem ini adalah untuk mencegah berbagai jenis serangan siber dengan pendekatan yang adaptif. Sistem memanfaatkan *IPS* untuk mendeteksi dan menghentikan serangan secara aktif, serta menggunakan *machine learning* dalam menganalisis paket data jaringan. Selain itu, sistem juga terintegrasi dengan Wazuh sebagai platform *SIEM* agar informasi keamanan jaringan dapat di-*monitor* dan diringkas secara menyeluruh.

1.5 Batasan Tugas Akhir

Batasan pada tugas akhir dijabarkan sebagai berikut:

1. Sistem tidak memblokir serangan secara otomatis, melainkan hanya mendeteksi dan mengumpulkan log.
2. Fungsi Snort hanya digunakan untuk *capture* dan meneruskan paket, tanpa *rules signature* aktif.
3. Model *machine learning* hanya mengenali lima label yaitu normal, dos, probe, r2l, dan u2r.
4. Integrasi ke Wazuh hanya mengirim log satu arah, tanpa feedback atau otomatisasi.
5. Sistem diuji dalam jaringan lokal, belum diimplementasikan untuk skala besar.
6. Model Machine Learning tidak di-*tuning* secara detail.
7. Fokus terhadap integrasi antara IPS dengan Machine Learning.

1.6 Metodologi

Adapun metodologi pada penelitian Tugas Akhir ini, sebagai berikut.

1. Studi Literatur

   Melakukan riset penggunaan beberapa komponen perangkat lunak yang diimplementasikan, dengan mengumpulkan beberapa paper dan jurnal perangkat lunak yang sudah ditentukan, sehingga kami mendapatkan informasi terkait penggunaan perangkat, hal ini menyangkut IPS sebagai pemeriksa log atau *scanner log*, Machine Learning sebagai *decision maker* dan SIEM sebagai perangkat monitoring jaringan pada sistem.

2. Pengumpulan Komponen

   Penentuan komponen perangkat lunak yang digunakan saat merancang sistem pada Tugas Akhir, dengan membandingkan beberapa kemampuan perangkat lunak, berdasarkan hasil riset studi literatur, seperti kecocokan pada sistem dan tingkat kesulitan pemakaian perangkat lunak untuk diimplementasikan.

3. Perencanaan Sistem

   Perencanaan dilakukan dengan melakukan percobaan pada perangkat lunak dan mencoba merancang beberapa kemungkinan bentuk dari sistem yang dibuat, pada tahap ini kami membandingkan perangkat lunak sesuai dengan studi literatur dan perencanaan yang sudah biasa dilakukan oleh beberapa *engineer team,* sehingga dapat kemudahan kami dalam membuat konsep *design* kami, dan mendapatkan bentuk sistem yang optimal.

4. Simulasi Perencanaan

   Simulasi perencanaan diawali dengan instalasi software pada masing-masing perangkat anggota tim sesuai pembagian tugas. Setelah seluruh komponen terpasang, dilakukan integrasi antara IPS dan machine learning, di mana model machine learning bertugas mengidentifikasi serangan, dan IPS menangani serangan yang telah terdeteksi. Sistem kemudian digabungkan dengan platform SIEM untuk menyediakan monitoring jaringan secara real-time.

5. Analisis Perencanaan

   Analisis perencanaan didapatkan dengan cara melihat hasil pada sistem, dan dibandingkan kinerjanya setara bertahap, kedua dari Virtual Machine akan menyerang (VM RED) dan bertahan (VM BLUE), pada VM RED sebagai penyerang, menggunakan serangan random dengan menggunakan pola yang berbeda, sementara VM BLUE sebagai target ditanamkan sistem pertahanan seperti SIEM dan Snort untuk me-*monitoring* jaringan yang dipakai.