BAB I
PENDAHULUAN

1.1 Latar Belakang

Era digitalisasi yang semakin maju membuat keamanan sistem menjadi aspek yang paling krusial seiring dengan ancaman siber yang semakin canggih dan kompleks. Dalam jaringan organisasi yang besar, penyusupan sering terjadi ke dalam jaringan komputer yang berasal dari *hacker* dan *cracker*, pihak tersebut terkadang menggunakan berbagai serangan untuk menghambat kelancaran operasi jaringan (Bada et al., 2020). Melalui serangan siber yang dapat mendatangkan kerugian, maka perangkat harus dilindungi dari semua jenis serangan siber yang tidak diinginkan dan tidak sah (Akhriana & Irmayana, 2020). Dalam menjaga keamanan perangkat jaringan, diperlukan sistem deteksi ancaman yang dapat digunakan untuk mengidentifikasi, mendeteksi potensi serangan atau aktivitas yang mencurigakan pada jaringan (Hu et al., 2020). Oleh karena itu penting menjaga perangkat jaringan sebagai hal yang krusial dan sebagai salah satu bentuk tindakan untuk menjaga perangkat jaringan dengan menerapkan *Intrusion Detection* (Mishra & Smirnova, 2021).

Menurut *National Institute of Standard and Technology* (NIST) deteksi intrusi merupakan proses pemantauan insiden yang terjadi dalam sistem komputer atau jaringan dengan menganalisis peristiwa-peristiwa atau insiden yang terjadi untuk mencari tanda adanya penyusupan. Sebagai perlindungan terhadap ancaman siber yang terus berkembang, *Intrusion Detection System* (IDS) merupakan solusi untuk melindungi perangkat dengan cara mendeteksi sedini mungkin serangan siber yang berpotensi menyebabkan kerusakan lebih lanjut pada pihak yang menjadi target dari serangan siber. IDS merupakan sistem keamanan jaringan yang efektif untuk mendeteksi arus lalu lintas jaringan yang mencurigakan, dan IDS memiliki dampak yang signifikan dalam mekanisme keamanan jaringan untuk melindungi jaringan komputer (Kumar et al., 2021).

IDS perlu diimplementasikan pada setiap lingkungan jaringan, karena IDS dapat mengidentifikasi secara efektif perilaku abnormal di lingkungan jaringan yang kompleks, dan IDS merupakan metode yang efektif untuk memastikan

keamanan pada jaringan komputer (Wang et al., 2021). Dalam banyaknya serangan siber yang ada, serangan DDoS merupakan salah satu serangan siber yang paling sering ditemui dan merusak (Chovanec et al., 2023), dan serangan PS sangat umum digunakan *hacker* untuk mencari *port* mana saja yang rentan terhadap serangan eksploitasi (Nisa & Kifayat, 2020). Hal ini yang membuat IDS diharuskan menjadi solusi yang efektif dan efisien dalam mendeteksi intrusi dengan skala yang besar (Mishra & Smirnova, 2021).

Terdapat dua jenis utama teknologi IDS yaitu *Host-based Intrusion Detection System* (HIDS) dan *Network-based Intrusion Detection System* (NIDS). Pada HIDS, deteksi hanya dapat dilihat dari satu sistem komputer dan berkas penting dari komputer yang dipasang IDS. Oleh karena itu, jenis serangan yang tersebar di jaringan sulit untuk dideteksi oleh HIDS. Dalam NIDS, informasi berbahaya dapat dideteksi dari interkoneksi komputer yang beragam, dan NIDS dapat ditempatkan pada *router* atau *switch* dalam jaringan (Kumar et al., 2021). Sehingga, pada penelitian ini akan menerapkan NIDS untuk mengamankan perangkat jaringan, dikarenakan pengguna perlu mendeteksi lebih dini apabila terjadi serangan atau anomali pada jaringan untuk menghindari kerusakan berlebih yang tidak diinginkan, serta pada penelitian ini akan membandingkan *tools* NIDS mana yang terbaik dengan parameter yang ditentukan.

Berdasarkan penelitian yang dilakukan oleh Hoover & Thompson (2022) dilakukan studi perbandingan IDS *Snort* 3 dan *Suricata* dengan mempertimbangkan performa *alert* dan *resource utilization*. Hasil penelitian tersebut menunjukan bahwa kedua sistem tersebut sangat mirip dalam hal penggunaan *Central Processing Unit* (CPU) *usage* yang setara, tetapi *Suricata* lebih boros dalam penggunaan *memory* daripada *Snort*. Mengenai perilaku peringatan, *Suricata* mendeteksi lebih banyak serangan dan memperingatkan 2 kali dan 3,5 kali lebih banyak dari pada *Snort* 3. Pada penelitian yang dilakukan oleh Bada dkk (2020) melakukan analisis perbandingan kinerja *open-source* IDS yaitu *Snort* 2, *Suricata* dan *Bro*. Dalam analisisnya peneliti mempertimbangkan efektivitasnya dalam mendeteksi *Denial of Service* (DoS) , *probe*, *scan*, serangan *user-to-local* dan *user-to-root* dan juga akurasi deteksi dengan parameter *confusion Matrix* yang diantaranya yaitu *False Positive Rate* (FPR), *False Negative Rate* (FNR), *True*

Positive Rate (TPR) pada lingkungan virtual. Hasil penelitian tersebut menunjukan *Snort* 2 lebih baik dari *Suricata* dan *Bro* dalam hal akurasi deteksi intrusi.

Pada penelitian yang dilakukan oleh Lukman & Suci (2020), dilakukan analisis perbandingan kinerja IDS *Snort* 2 dan *Suricata* dalam mendeteksi serangan DoS *Synchronize* (SYN) *flood* dengan memperhatikan parameter jumlah deteksi serangan, CPU *usage*, *memory usage,* dan efektivitas deteksi serangan. Hasil penelitian tersebut menunjukan bahwa *Snort* lebih unggul dalam pendeteksian serangan, penggunaan CPU *usage*, dan fitur informasi data serangan. Sedangkan *Suricata* lebih unggul dalam efektivitas serangan dari data *uncaptured package* dan penggunaan *Random Access Memory* (RAM) *usage.* Kemudian, Pada penelitian yang dilakukan oleh Boukebous dkk (2023), dilakukan penelitian analisis komparatif *Snort 2, Snort 3* dan *Suricata* yang dilakukan pada lingkungan virtual. Parameter yang digunakan pada penelitian ini yaitu diantaranya CPU *usage*, RAM *usage*, *packet drop* dan *loss of alert* dengan menggunakan *case* serangan *Distributed Denial of Service* (DDoS). Hasil penelitian ini menyimpulkan bahwa *Snort 3* memiliki kinerja yang lebih baik daripada *Snort 2* dan *Suricata*.

Rujukan penelitian tersebut membuat peneliti merencanakan penelitian dengan judul "Analisis Perbandingan Performa *Intrusion Detection System* (IDS) Dalam Mendeteksi Serangan *Port Scanning* (PS) dan *Distributed Denial Of Service* (DDoS)". Meskipun penelitian sejenis sudah banyak dilakukan, penelitian sebelumnya belum berfokus pada IDS *tools* terbaru seperti *Snort* 3, *Suricata* serta *Zeek* dengan parameter yang lebih spesifik untuk membandingan IDS *tools*. Oleh karena itu, penelitian ini akan berfokus pada analisis perbandingan IDS *tools* yang di antaranya *Snort* 3, *Suricata,* dan *Zeek* terbaru, dengan mempertimbangkan parameter *confusion Matrix,* kecepatan deteksi serangan, dan *resource usage* terhadap berbagai jenis serangan PS dan DDoS.

1.2 Rumusan Masalah

Dari latar belakang di atas, maka peneliti dapat merumuskan masalah sebagai berikut:

1. Bagaimana analisis penggunaan IDS dalam mendeteksi serangan?
2. Bagaimana perbandingan performa IDS terhadap parameter *confusion matrix*, kecepatan deteksi serangan, dan *resource usage*?

1.3 Batasan Masalah

Berdasarkan rumusan masalah dan tujuan penelitian yang sudah dijelaskan, terdapat batasan masalah yang dapat dijelaskan sebagai berikut:

1. Terdapat dua jenis utama teknologi IDS yaitu HIDS dan NIDS, pada penelitian ini peneliti berfokus pada NIDS.
2. NIDS *tools* yang digunakan pada penelitian ini yaitu *open-source* NIDS *tools* diantaranya: *Snort* 3, *Suricata*, dan *Zeek.*
3. Parameter yang digunakan pada penelitian ini yaitu *confusion matrix* yang terdiri dari TPR, FPR, *True Negative Rate* (TNR), FNR, kemudian kecepatan deteksi serangan, dan *resource usage* yang didalamnya terdiri dari CPU *usage*, *memory usage* dan *network usage*.
4. Terdapat banyak jenis serangan, pada penelitian ini serangan yang digunakan adalah DDoS, dan PS.
5. Penelitian dilakukan melalui lingkungan virtual menggunakan *virtual box.*

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah dan batasan masalah, terdapat beberapa tujuan dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Menganalisis penggunaan IDS dalam mendeteksi serangan.
2. Membandingkan performa IDS dalam mendeteksi serangan berdasarkan parameter *confusion matrix*, kecepatan deteksi serangan, dan *resource usage*.

1.5 Manfaat Penelitian

Terdapat banyak manfaat penelitian yang akan dilakukan, oleh karena itu mengenai penjelasan lebih terperinci akan dijelaskan sebagai berikut sesuai klasifikasinya :

1.5.1 Manfaat Teoritis

Secara teoritis hasil penelitian ini diharapkan dapat bermanfaat, sebagai sumbangsih pemikiran bagi para peneliti-peneliti berikutnya untuk menjadi pijakan penelitian dan menjadi referensi pada penelitian-penelitian berikutnya yang berhubungan dengan penelitian IDS.

1.5.2 Manfaat Praktis

Penelitian ini diharapkan mampu memberikan pengetahuan dan kontribusi kepada pihak sebagai berikut :

1. Bagi Penulis manfaat penelitian secara praktis dapat menambah wawasan mengenai pentingnya IDS.
2. Bagi Masyarakat manfaat penelitian secara praktis diharapkan dapat menambah wawasan mengenai pentingnya mendeteksi lebih dini ancaman intrusi dari serangan jaringan.
3. Bagi Perusahaan manfaat penelitian secara praktis diharapkan dapat menjadi solusi bagi perusahaan untuk mengetahui IDS *tools* terbaik dalam mendeteksi serangan.

1.6 Struktur Organisasi Skripsi

Penelitian ini terdiri dari lima bab seperti yang tercantum dalam Pedoman Penulisan Karya Ilmiah UPI Tahun 2021. Bab I Pendahuluan, Bab II Kajian Pustaka, Bab III Metode Penelitian, Bab IV Temuan dan Pembahasan, dan Bab V Simpulan, Implikasi, Rekomendasi.

1. Bab I Pendahuluan, pada bab ini akan dideskripsikan mengenai gambaran awal penelitian dengan struktur latar belakang penelitian tentang topik dan isu yang diangkat di dalam penelitian secara menarik dan sesuai dengan perkembangan masalah penelitian yang akan diteliti, tujuan penelitian menyatakan cerminan perumusan permasalahan yang disampaikan sebelumnya, manfaat penelitian merupakan nilai lebih dan kontribusi yang dihasilkan di dalam penelitian, dan struktur organisasi memuat sistematis penulisan skripsi dengan memberikan gambaran kandungan pada setiap bab, urutan penulisan, serta keterkaitan antara satu bab dengan bab lainnya dalam membentuk suatu kerangka untuk skripsi.
2. Bab II Kajian Pustaka, pada bab ini akan mendeskripsikan hal-hal berikut: (1) konsep-konsep, teori-teori, dalil-dalil, hukum, model, rumus utama serta turunan bidang yang dikaji; (2) penelitian terdahulu yang relevan dengan bidang yang diteliti seperti prosedur, subjek dan temuannya; dan (3) posisi teoritis peneliti yang berkenaan dengan masalah yang diteliti.
3. Bab III Metode Penelitian, pada bab ini berisi bagian yang bersifat *procedural* yang akan mengarahkan pembaca untuk mengetahui bagaimana peneliti merancang dan menyusun alur penelitian yang dimulai dengan pemilihan

pendekatan, instrumen, teori pengumpulan data, hingga langkah-langkah analisis yang akan diterapkan di dalam sebuah penelitian.

4. Bab IV Temuan dan Pembahasan, pada bab ini akan diuraikan dan mendeskripsikan mengenai temuan penelitian berdasarkan hasil pengolahan dan analisis data dengan berbagai kemungkinan sesuai dengan urutan rumusan masalah dan tujuan penelitian yang telah dirancang sebelumnya.
5. Bab V Penutup, bagian ini terdiri dari sub-judul kesimpulan, dan saran dengan menyajikan penafsiran dan pemaknaan peneliti terhadap hasil analisis temuan penelitian.