BAB I

PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer merupakan sebuah sistem yang terdiri dari komputer-komputer yang di desain untuk dapat berbagi sumber daya (Sudirman & Akma Nurul Yaqin, 2021). Keamanan jaringan komputer tentunya menjadi masalah yang harus dihadapi ketika memutuskan memulai akses informasi secara online, terlebih jika berhubungan dengan data sensitif yang dapat mempengaruhi kinerja dan reputasi (Sudirman & Akma Nurul Yaqin, 2021), tujuannya adalah untuk mengantisipasi resiko jaringan komputer yang berupa ancaman fisik maupun logik (Dwinanto & Setiyani, n.d., 2021). Sistem harus dilindungi dari semua jenis serangan dan upaya penyusupan oleh orang yang tidak berhak Pitriyanti, *et al.* (2023). Tujuannya yaitu untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung mengganggu aktifitas dalam jaringan komputer (Yanto, 2020).

Audit keamanan merupakan proses pengumpulan bukti untuk mengevaluasi keamanan sistem secara keseluruhan termasuk kebijakan, prosedur, kontrol, dan infrastruktur teknologi informasi Algiffary *et al.* (2023). Audit ini bertujuan untuk memastikan bahwa sistem memenuhi kebutuhan keamanan organisasi dan meminimalkan resiko keamanan sistem informasi Algiffary *et al.* (2023). Kejahatan cyber selalu berhubungan dengan teknologi informasi dan komputer Adam Zukhruf *et al.* (2023). Salah satu tindak kejahatan pada jaringan komputer adalah serangan *Distributed Deniel of Service* (DDoS) Feronika Nainggolan *et al.* (2022). DDoS merupakan sebuah percobaan penyerangan dari beberapa sistem komputer yang menargetkan sebuah server agar jumlah *traffic* menjadi terlalu tinggi sampai server tidak bisa menghendel *request* Santoso *et al.* (2021). Berbagai macam serangan DDoS diantaranya ICMP *flooding* (*ping of death*), TCP *flooding* dan UDP *flooding* (Purba & Efendi, 2020). DDoS yang paling sering digunakan adalah *ping of deadth*, dimana

penyerang memanfaatkan komunikasi ICMP untuk dibanjiri oleh paket data yang diminta, sehingga membuat sistem server menjadi lambat Feronika Nainggolan *et al.* (2022). Serangan DDoS saat ini menargetkan layanan yang spesifik, sehingga target akan menjadi down (Nisa & Ramadona, 2023). Serangan DDoS mempengaruhi korban dalam bentuk menemukan bug atau kelemahan untuk mengganggu layanan atau menghabiskan semua *bandwidth* sumber daya dari sistem korban (Nurbahri & Widi Nurcahyo, 2023). Oleh sebab itu solusi yang digunakan yaitu dengan dibutuhkannya rancangan sistem yang dapat menjaga jaringan itu sendiri. Sistem jaringan harus dilengkapi dengan sistem yang dapat mendeteksi penyusupan atau intrusi (*intrusion*) Feronika Nainggolan *et al.* (2022).

Sistem tersebut dikenal dengan *snort*. *Snort* merupakan sebuah aplikasi keamanan jaringan yang berfungsi dalam mendeteksi adanya ancaman dalam jaringan komputer, seperti penyusup, pemidaian, maupun penyerangan (Purba & Efendi, 2020). Snort merupakan tools yang berbasis *Intrusion Detection System* (IDS) yang dapat memonitor jaringan yang berdampak serangan dan menyimpan serangan pada log Feronika Nainggolan *et al.* (2022).

Intrusion Detection System (IDS) merupakan sistem yang mendeteksi dan mencegah tindakan yang dilakukan dengan tujuan merusak komputer dan jaringan komputer (Khatib Sulaiman & Polatgil, 2022.). Dalam mengamankan jaringan komputer, metode IDS dapat mengoptimalkan tingkat keamanan jaringan komputer untuk mendeteksi adanya serangan sehingga administrator segera melakukan tindakan pencegahan Meli Pitriyanti *et al.* (2021). IDS mampu mendeteksi serangan sesusai dengan rule yang dibuat dan memberikan penanganan serangan sesuai dengan aksi yang dilakukan oleh administrator Rudi Suwanto *et al.* (2019).

Penelitian yang dilakukan oleh Raihan *et al.* (2023) dengan judul "Sistem Keamanan Jaringan Komputer Berbasis Teknik *Intrusion Detection System* (IDS) untuk mendeteksi Serangan *Distributed Deniel of Service* (DDOS)" merancang sebuah sistem keamanan jaringan komputer berbasis *Intrusion Detection System* menggunakan *snort* dan *portsentry* dapat mendeteksi dan mencegah serangan DDOS seperti ping icmp, nmap, dan DDOS. Hasil pengujian dari penerapan *Intrusion Detection System* menggunakan *snort* dan *portsentry* yaitu serangan dapat dideteksi dan dicegah sehingga grafik *network history* dan penggunaan *memory* sebelum diterapkan *snort* dan *portsentry* pada saat dilakukan serangan DDOS *traffic* jaringan

mencapai 80.0 MB/s penggunaan *memory* naik 40% dan penggunaan CPU 60% dan setelah diterapkan *snort* dan *portsentry* pada saat melakukan serangan *ping icmp, nmap*(port scan), dan DDOS serangan dapat di blokir dan *traffic* jaringan normal dengan *traffic* 205 bytes/s, pemakaian CPU 20% dan pemakaian momory 20%. Kesimpulan dari penelitian ini dengan menerapkan teknik keamanan jaringan *Intrusion Detection System* berdasarkan hasil pengujian serangan *ping icmp, nmap*(port scan), dan DDOS serangan dapat dideteksi dengan mengimpementasikan *snort* dan serangan dapat dicegah dengan mengimplementasikan *portsentry*.

Penelitian yang dilakukan oleh Hasri & Aggy (2023) dengan judul " Implementasi *Intrusion Detection Prevention System* Sebagai Sistem Keamanan Jaringan Komputer Kejaksaan Negeri Pariaman Menggunakan *Snort* dan *IPTables* Berbasis Linux" melakukan penerapan *IDS Snort* pada server dapat mendeteksi sebuah serangan atau gangguan pada server dan secara efektif dapat bekerja sebagai keamanan jaringan komputer. Hasil pengujian dan penerapan *Intrusion Detection System* menggunakan *Snort* sebelum adanya serangan *Ping of Deadth* tampilan grafik *network* yang ditampilkan server masih terlihat normal dengan total *receiving* sebesar 30,5 MiB dan total *sending* 20,4 MiB, setelah terjadi serangan terjadi kenaikan yang signifikan pada grafik *network*, dengan total *receiving* sebesar 54,9 GB dan total *sending* sebesar 24,9GB. Setelah diterapkan aturan *IPS Iptables* ip penyerang berhasil di blokir dan tidak dapat melakukan penyerangan kembali terhadap server dan grafik *network* kembali normal. Pada saat dilakukan pengujian kualitas layanan server dengan metode QoS (*Quality of Service*) untuk menguji kecepatan *upload* dan *download* pada server diperoleh upload sebesar 94,0 Mbit dab download 95,2 Mbit sebelum terjadi serangan dengan nilai index rata-rata 4 pada parameter *throughput, delay, jitter,* dan *packet lost* dengan kategori sangat baik. Setelah terjadi serangan kulalitas layanan server menurun sebanyak 50% dengan nilai index rata-rata 2 dengan kategori sedang. Dengan diterapkannya *IDS Snort* dan aturan *Iptables* pada server jaringan server kembali membaik dengan nilai index rata-rata 3,75 dengan kategori baik. Kesimpulan dari penelitian ini dengan menerapkan *IDS Snort* dan *IPS Iptables* pada server dapat dilakukan deteksi sebuah serangan dan gangguan pada server dan secara efektif dapat bekerja sebagai keamanan jaringan komputer dan dapat memulihkan kualitas layanan server dalam sebuah jaringan dengan index rata-rata sebesar 3,75 dari nilai index sebesar 4.

Pada Penelitian yang dilakukan oleh Tri & Adam (2022) dengan judul "Pemanfaatan *Network Forensic Infestigation Framework* untuk Mengidentifikasi Serangan Jaringan Melalui *Intrusion Detection System* (IDS)" melakukan penerapan *IDS Snort* pada komputer server dapat mendeteksi aktivitas serangan *network scanning* dan serangan DOS *Ping of Deadth* secara efektif dengan memberikan *alert* pada administrator. Hasil pengujian dan penerapan *Intrusion Detection System* menggunakan *snort* dapat mendeteksi serangan *ping of deadth* oleh komputer dengan ip 192.168.56.103 dengan mengirim paket sebanyak 217406 kali dengan durasi 11 menit 42 detik dengan mengirimkan paket sebesar 13180928 *bytes* atau sekitar 206 MB yang di indikasikan *packet flooding*. kesimpulan dari penelitian ini *Intrusion Detection System* efektif mendeteksi adanya aktifitas *network scanning* dan serangan DOS *Ping of deadth* dengan memberikan *alert* pada administrator karna melanggar rule pada IDS. catatan log IDS dapat mempermudah proses investigasi sehingga serangan dapat terlacak pada sumber serangan dan media serangan.

Penelitian yang dilakukan oleh Zahra *et al.* (2022) dengan judul " Analisis Keamanan Jaringan dari Serangan DoS Pada Sistem Inventaris Sanggar Tari Natya Lakshita Mengguakan IDS" melakukan penerapan *Intrusion Detection System* (IDS) *Snort* pada sistem inventaris sanggar tari Natya Lakshita dan berhasil mendeteksi serangan pada *port* 80 dengan ip 100.0.221.247 dan mengirimkan *alert* kepada administrator berupa log file. Dampak dari serangan yang dikirim mengakibatkan komputer menjadi *overload* sehingga penggunaan CPU mencapai 100%. Kesimpulan dari penelitian ini penerapan *Intrusion Detection system* mampu mendeteksi serangan yang dilakukan penyerang yang dilakukan pada *port* 80 dan mampu mendeteksi ip penyerang.

Pada penelitian yang dilakukan oleh Lukman & Melati (2020) dengan judul " Analisis Perbandingan Kinerja *Snort* dan *Surica* Sebagai *Intrusion Detection System* Dalam Mendeteksi Serangan *Syn Flood* Pada Web Server Apache" melakukan analisis perbandingan kinerja *Snort* dan Surica dalam mendeteksi serangan *Deniel of Service Syn Flood* dengan parameter acuan jumlah serangan yang terdeteksi dan efektifitas deteksi serangan. Hasil pengujian dan analisis didapatkan dengan melakukan 30 kali pengujian IDS *Snort* lebih banyak melakukan pendeteksian dibandingkan dengan IDS *Surica* dengan rata-rata performa sebanyak 84,97% dan memiliki standar deviasi 167248,43 dibandingkan IDS *Surica* sebanyak 74,62% dengan setandar deviasi

128160,39. Pada parameter penggunaan *resource* CPU *Snort* lebih unggul dibandingkan IDS *Surica* dengan rata-rata rasio penggunaan CPU sebanyak 78,31% dibandingkan dengan IDS Surica 80,08%. Dari segi fitur *Snort* lebih unggul karna dapat menampilkan informasi data serangan dan data *outstanding* paket secara langsung, sedangkan surica harus membuka file log terlebih dahulu untuk melihat informasi serangan dan tidak memiliki informasi data *outstanding*. Kesimpulan dari penelitian ini bahwa IDS *Snort* lebih unggul dalam pendeteksian serangan, penggunaan *resource* CPU, dan fitur informasi data serangan dibandingkan dengan *Surica*.

Keamanan jaringan komputer menjadi isu yang sangat penting, terutama pada institusi pendidikan. SMKS YPPI Tualang merupakan salah satu sekolah swasta yang terletak di Kecamatan Tualang Provinsi Riau yang merupakan program CSR dari PT Indah Kiat *Pulp and Paper Tbk*. SMKS YPPI memiliki tiga konsentrasi keahlian yaitu Teknik Mekanik Industri, Teknik Otomasi Industri dan Teknik Komputer Jaringan dan Telekomunikasi. Dalam kegiatan belajar mengajar dan operasional sekolah SMKS YPPI Tualang bergantung pada infrastruktur teknologi informasi dalam mendukung kegiatan belajar mengajar. salah satu ancaman keamanan jaringan yang sering dihadapi yaitu serangan *Distributed Deniel of Service* (DDoS). Serangan DDoS dapat mengekibatkan jaringan komputer dan server menjadi tidak dapat diakses dan mengganggu aktivitas belajar mengajar dan operasional sekolah yang mengakibatkan kerugian waktu dan biaya.

Berdasarkan hal tersebut maka perlu dilakukannya audit pada keamanan jaringan untuk dapat mendeteksi celah keamanan dan kerentanan yang terjadi pada jaringan untuk meningkatkan perlindungan terhadap infrastruktur teknologi informasi yang digunakan. Audit keamanan jaringan komputer bertujuan untuk mengidentifikasi dan menganalisa potensi celah keamanan serta kerentanan yang dapat dimanfaatkan oleh penyerang untuk melancarkan serangan DDoS. Dengan menggunakan *Snort Intrusion Detection System* (IDS), penelitian ini akan melakukan evaluasi terhadap efektifitas *Snort* dalam mendeteksi dan mencegah serangan DDoS pada jaringan komputer server SMKS YPPI Tualang. Berdasarkan hal tersebut dan studi sebelumnya, maka penelitian ini akan diangkat kedalam bentuk thesis dengan judul "**Audit keamanan jaringan Komputer Server dari serangan *Distributed Deniel of Service* (DDoS) menggunakan *Snort Intrusion Detection System* (IDS)"**. Dengan

penelitian ini diharapkan mampu mendeteksi dan menganalisa celah keamanan pada jaringan komputer server SMKS YPPI Tualang sehingga dapat mencegah terjadinya serangan DDoS pada jaringan komputer.

1.2 Perumusan Masalah

Berdasarkan masalah yang ada dalam penelitian ini sesuai dengan uraian yang ada pada latar belakang, maka penulis merumuskan beberapa perumusan masalah yang akan dibahas pada penelitian ini, yaitu :

1. Bagaimana cara mengidentifikasi dan mendeteksi serangan *Distributed Denial of Service* (DDoS) pada jaringan komputer SMKS YPPI Tualang?
2. Bagaimana Penerapan Audit Keamanan Jaringan Menggunakan *Snort Intrusion Detection System* dapat mengurangi kerentanan Keamanan pada jaringan komputer server SMKS YPPI Tualang ?
3. Bagaimana efektifitas *Snort Intrusion Detection System* (IDS) dalam mendekteksi dan merespon serangan DDoS ?
4. Bagaimana pengaruh serangan DDoS terhadap layanan dan kinerja jaringan komputer server SMKS YPPI Tualang ?

1.3 Batasan Masalah

Agar pembahasan pada penelitian ini tidak menyimpang, berlatar belakang dari masalah yang dipaparkan, maka peneliti membatasi ruang lingkup objek penelitian. Ruang lingkup penelitian ini sebagai berikut :

1. Penelitian ini difokuskan pada jaringan komputer server di SMKS YPPI Tualang di Kabupaten Siak, Provinsi Riau.
2. Metode yang digunakan pada penelitian ini adalah *Intrusion Detecsion System* (IDS) dengan tool aplikasi yang digunakan yaitu *snort*.
3. Pengujian simulasi serangan DDoS yang dilakukan hanya pada serang *ping of deadth, Flooding, dan Smurf.*

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai pada penelitian ini untuk mencapai beberapa sasaran penting yang diharapkan dapat memberikan manfaat jangka panjang bagi pihak yang terlibat agar bermanfaat kedepannya. Adapun tujuan pada penelitian ini adalah sebagai berikut:

1. Mengidentifikasi dan mendeteksi serangan DDoS pada jaringan komputer yang mencakup pola-pola serangan, analisis lalu lintas dan jenis serangan pada jaringan.
2. Menguji kinerja *Snort* IDS dalam mendeteksi serangan DDoS dan mengukur efektifitas dalam mengurangi kerentanan keamanan jaringan.
3. Mengukur efektifitas *Snort* IDS dalam mendeteksi dan merespon serangan DDoS yang mencakup pada pengujian dalam skenario beberapa serangan.
4. Menganalisis dampak serangan DDoS terhadap layanan dan kinerja jaringan komputer yang mencakup efek serangan yang ditimbulkan terhadap jaringan, penurunan kinerja, dan pengukuran *downtime*.

1.5 Manfaat Penelitian

Penelitian yang dilakukan diharapkan dapat memberikan manfaat dan kontribusi pada bidang yang diteliti, dengan harapan temuan dan hasil yang didapatkan bermanfaat bagi akademisi, praktisi, dan pembuat kebijakan. Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Bagi peneliti dapat menambah wawasan dalam hal analisis keamanan jaringan komputer dari serangan DDoS menggunakan metode *snort intrusion detection system* (IDS)
2. Bagi pendidikan dapat memberikan kontribusi pemikiran mengenai keamanan jaringan komputer khususnya mengenai serangan DDoS pada jaringan komputer. Selain itu juga dapat menjadi salah satu sumber informasi atau referensi untuk penelitian lainnya dibidang keamanan jarigan komputer.

3. Bagi sekolah dapat menjaga dan memonitoring keamanan jaringan, khususnya keamanan jaringan komputer server dari serangan DDoS.

1.6 Sistematika Penulisan

Sistematika dalam penulisan tesis ini mencakup berbagai bagian penting untuk disertakan dalam sebuah tesis yang terstruktur dengan baik. Setiap bagian dari tesis ini akan diuraikan secara rinci mulai dari pendahuluan, landasan teori, metodologi penelitian, Analisa dan perancangan, implementasi dan pengujian, hingga penutup yang berisi Kesimpulan dan saran. Dengan penjabaran yang komprehensif ini, diharapkan pembaca dapat memahami alur penelitian dan kontribusi ilmiah yang diberikan pada tesis ini. Sistematika dalam penulisan tesis ini dapat di jabarkan sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini menjelaskan mengenai latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan dari keseluruhan bab yang akan dibuat dalam penelitian ini.

BAB II LANDASAN TEORI

Pada bab ini berisi tentang Kumpulan litelatur dari jurnal, artikel, tugas akhir, makalah, dan lainnya yang berkairan dengan tesis.

BAB III METODOLOGI PENELITIAN

Pada bab ini berisi tentang kerangka kerja perangkat penelitian yang digunakan, mekanisme dan prosedural dalam Audit jaringan komputer server dari serangan *Disteibuted Deniel of Services* (DDoS) menggunakan *Snort Intrusion Detection System* (IDS).

BAB IV ANALISA DAN PERANCANGAN

Pada bab ini berisi tentang analisis terhadap Audit jaringan komputer server dari serangan *Disteibuted Deniel of Services* (DDoS) menggunakan *Snort Intrusion Detection System* (IDS).

BAB V IMPLEMENTASI DAN PENGUJIAN

Pada bab ini berisi tentang pengujian terhadap hasil penelitian, implementasi, dan analisis hasil.

BAB VI PENUTUP

Pada bab ini berisi kesimpulan dan saran.