BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Pada zaman sekarang ini internet adalah salah satu hal terpenting di dalam kehidupan dan gaya hidup masyarakat di seluruh dunia. Berdasarkan data yang diberikan oleh APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), jumlah pengguna internet di Indonesia pada tahun 2023 adalah sebanyak 215 juta pengguna. Memasuki tahun 2024 pada triwulan I (satu) jumlah pengguna internet terus mengalami peningkatan hingga menyentuk angka 221 juta pengguna [1]. Berdasarkan informasi tersebut maka dalam waktu kurang dari 3 bulan pertama jumlah pengguna internet di Indonesia mengalamin peningkatan sebesar 6 juta pengguna (APJII, 2024).

Dari besarnya jumlah pengguna tersebut, maka semakin besar juga tingkat kejahatan siber di internet. Berdasarkan *website* dari Data Indonesia melalui laporan dari BSSN (Badan Siber dan Sandi Negara) pada tahun 2023 jumlah serangan siber di Indonesia tercata sebanyak 279,84 juta serangan siber [2]. Hal ini mengindikasikan bahwa, terdapat lebih dari satu kali serangan siber pada setiap jumlah pengguna internet di Indonesia. Adapun jenis serangan yang digunakan seperti *Generic Trojan RAT Activity, Advanced Persisten Threat* (APT), *malware,* dan *Denial of Service* (DOS). Serangan *Denial of Service* (DoS) merupakan jenis serangan terhadap sistem dalam jaringan internet dengan cara menghabiskan *resource* yang dimiliki oleh suatu sistem sehingga tidak dapat menjalankan fungsinya dengan benar dan secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan sistem yang diserang tersebut.

Di dalam sejarah perkembangan internet di dunia, terdapat beberapa kejahatan siber yang menggemparkan dunia yang salah satunya adalah serangan DDoS tersebut [3]. Serangan tersebut di antaranya terjadi pada situs CNN. Pada tahun 2014 CNN yang merupakan salah satu situs berita terkemuka mengalami serangan DDoS yang besar dengan menggunakan botnet untuk membanjiri server dengan permintaan HTTP. Akibatnya, situs CNN menjadi lambat dan tidak dapat diakses yang mengakibatkan

rusaknya citra dan kredibilitasnya. Lalu pada tahun 2018, GitHub juga mengalami serangan DDoS yang besar dengan menggunakan ribuan perangkat terinfeksi untuk membanjiri server dengan lalu lintas berkecepatan tinggi. Serangan ini mengakibatkan gangguan layanan, menyulitkan pengguna dalam mengakses dan berkolaborasi pada proyek *open source*. Di Indonesia juga tidak lepas dari sejarah serangan DDoS yang cukup menggemparkan yang salah satunya adalah DDoS pada KasKus. Serangan ini terjadi pada tahun 2017 dimana KasKus merupakan forum *online* besar di Indonesia. KasKus mengalami serangan DDoS dimana pelaku menggunakan botnet yang membanjiri server dengan permintaan berlebihan. Akibatnya situs KasKus tidak dapat diakses yang berakibat mengganggu komunitas *online* dan partisipasi pengguna. Berdasarkan laporan dari Vida yang merupakan layanan penyedia keamanan identitas digital menyebutkan bahwa serangan DDoS yang terjadi di Indonesia mengalami peningkatan sebesar 40% pada tahun 2023 dan diprediksi serangan ini berpotensi akan terus meningkat pada tahun 2024

Suatu arsitektur jaringan komputer dihubungkan dengan menggunakan media gelombang elektromagnetik untuk melakukan transmisi data. (Irawan, 2013). Jaringan *Local Area Network* tanpa kabel disebut sebagai *Wireless Local Area Network* atau WLAN. Sedangkan Wi-Fi yang merupakan singkatan dari *Wireless-Fidelity* adalah sekumpulan standar yagn digunakan dalam penerapan *Wireless Local Area Network* (WLAN). Selain digunakan sebagai akses internet, Wi-Fi juga dapat digunakan untuk membuat jaringan tanpa kabel pada sebuah organisasi maupun instansi tertentu. (Priantama, 2015). Namun, di dalam penggunaannya Wi-Fi sebagai teknologi dari WLAN juga memiliki beberapa celah keamanan seperti LAN dengan kabel. Pihak yang tidak bertanggung jawab dapat menyusup ke jaringan WLAN dengan memiliki identitas IP *Address* maupun *port* sasaran yang terbuka.

Snort IPS (*Intrusion Prevention System*) adalah sebuah perangkat lunak yang digunakan untuk mendeteksi sekaligus memberikan penanganan serangan jaringan termasuk serangan DoS, *port scan*, dan *worm* yang beredar melalui jaringan. Snort dapat menangkap paket data jaringan dan menganalisisnya terhadap aturan-aturan yang didefinisikan oleh pengguna. (Stephen Northcutt, 2001). Snort merupakan tools yang dikenal luas dan digunakan oleh seorang profesional keamanan siber di seluruh dunia yang bertujua untuk mendeteksi dan mencegah intrusi jaringan, termasuk

serangan DDoS. Fleksibilitas dan kompatibilitas Snort dengan berbagai sistem operasi yang digunakan untuk menjalankannya membuatnya menjadi pilihan populer di kalangan ahli keamanan siber.

Berdasarkan latar belakang dan beberapa fenomena yang terjadi dari studi kasus di atas, penelitian ini bertujuan untuk mengetahui tingkat kerentanan keamanan jaringan *Wireless* LAN agar dapat segera dideteksi dan antisipasi dari bahaya serangan kemanan jaringan. Dari penjelasan yang telah dijabarkan, penulis akan melakukan penelitian terhadap subjek untuk mengidentifikasi dan menganalisis keamanan jaringan dengan menggunakan Snort dimana judul penelitian ini adalah "Simulasi Pencegahan Serangan *Denial of Service* Dengan Menggunakan Teknologi *Intrusion Prevention System* Berbasis Snort Terhadap Keamanan Jaringan *Wireless* LAN".

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijabarkan, maka rumusan masalah yang ditetapkan dalam penelitian ini, yaitu:

1. Bagaimana cara penerapan IPS Snort terhadap keamanan jaringan *Wireless* LAN sehingga dapat bekerja sebagai *monitoring* keamanan jaringan?
2. Bagaimana cara melakukan pencegahan terhadap keamanan jaringan *Wireless* LAN?
3. Bagaimana kelebihan dari penerapan IPS Snort terhadap keamanan jaringan *Wireless* LAN?

1.3. Batasan Masalah

Berdasarkan rumusan masalah yang telah dipaparkan, penulis membatasi masalah pada penelitian ini, yaitu:

1. Penggunaan *software* Snort untuk melakukan deteksi sekaligus serangan jaringan internet.
2. Metode yang digunakan dalam penelitian *Penetration testing* untuk melakukan pemindaian dan simulasi serangan terhadap jaringan.

3. Jenis serangan yang akan disimulasikan adalah *Denial of Service* berupa protokol TCP SYN *Flood*, UDP *Flood* dan kombinasi antara TCP SYN *Flood* dan UDP *Flood*.
4. Percobaan pemindaian dan simulasi serangan akan dilakukan 10 kali dalam waktu 60 detik dan 120 detik.
5. Sumber jaringan internet berasal dari *hotspot* seluler *smartphone*.
6. *Rules* yang dibuat hanya untuk mengatasi serangan TCP SYN *Flood* dan UDP *Flood*.

1.4. Tujuan Penelitian

Beberapa tujuan yang akan dicapai dari penelitian ini, yaitu:

1. Untuk mengetahui tentang cara penerapan IPS Snort terhadap keamanan jaringan *Wireless* LAN sehingga dapat bekerja sebagai *monitoring* keamanan jaringan.
2. Untuk mengetahui tentang cara melakukan pendeteksian sekaligus pencegahan terhadap keamanan jaringan *Wireless* LAN.
3. Untuk mengetahui kelebihan dari penerapan IPS Snort terhadap keamanan jaringan *Wireless* LAN.

1.5. Manfaat Penelitian

Berdasarkan rumusan masalah dan tujuan penelitian yang telah dipaparkan, maka manfaat dari penelitian ini, yaitu:

1. Menambah wawasan tentang pentingnya mengetahui dan mengantisipasi tingkat kerentanan kemanan jaringan dalam suatu lingkup khususnya dalam serangan *Denial of Service* yang memengaruhi performansi layanan lalu lintas jaringan.
2. Menambah wawasan tentang *software* maupun perangkat lain yang mampu digunakan sebagai alat untuk *monitoring* sekaligus pencegahan sebuah serangan yang dapat mengancam suatu kemanan jaringan dan simulasi yang dilakukan sebagai langkah dini dalam pencegahan tindak kejahatan siber.

3. Mendapatkan gambaran tentang bagaimana suatu sistem jaringan dapat dikatakan aman ataupun rentan terhadap serangan oleh pihak-pihak yang tidak bertanggungjawab.

1.6. Metodologi Penelitian

Metode yang dilakukan penulis untuk melakukan penelitian ini adalah dengan menggunakan metode:

1. Studi Literatur

   Metodologi ini dilakukan dengan mempelajari referensi bacaan dari buku-buku/literatur maupun jurnal ilmiah yang berkaitan dengan keamanan jaringan dan topik penelitian pada proyek akhir ini, seperti *software* IPS Snort dan metode pengujian keamanan jaringan yang dapat dilakukan.
2. Perencanaan

   Metodologi ini dilakukan dengan menyusun strategi dalam melakukan percobaan serangan serta rencana topologi yang akan dibangun untuk menerapkan kemampuan Snort dalam menahan skenario serangan dalam hal ini *Denial of Service.*
3. Uji dan Simulasi

   Tahapan pada metodologi ini dilakukan dengan simulasi langsung berdasarkan perencanaan yang telah disusun sesuai dengan target telah ditentukan.
4. Analisis Hasil

   Analisis hasil dilakukan setelah simulasi berhasil dilakukan dan telah mendapatkan data dari hasil kemampuan Snort dalam menahan serangan *Denial of Service*. Setelah semuanya dilakukan maka penulis akan membuat sebuah laporan final tentang topik penelitian proyek akhir yang telah dilakukan.

1.7. Sistematika Penulisan

Secara umum, sistematika penulisan proyek akhir ini terdiri dari beberapa bab dengan metode penyampaian sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II DASAR TEORI

Bab ini membahas tentang teori yang mendukung pengerjaan proyek akhir, seperti metode simulasi yang akan dilakukan dan prinsip kerja dari *software* IPS Snort agar dapat bekerja dalam mode *prevention* atau pertahanan terhadap serangan.

BAB III PERANCANGAN SISTEM

Bab ini membahas deskripsi perancangan dan simulasi topik proyek akhir, serta alur kerja yang dilakukan sesuai dengan skenario yang telah direncanakan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas tentang simulasi yang telah dilakukan dan analisis terhadap hasil simulasi.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil pengerjaan proyek akhir dan saran bagi para pembaca yang ingin mengembangkan atau modifikasi penelitian dengan topik proyek akhir yang sama dengan penulis.