BAB I
PENDAHULUAN

1.1 Latar Belakang

Indonesia menjadi salah satu negara yang memiliki jumlah pengguna internet terbesar di dunia. Data yang diterbitkan oleh datareportal.com dalam laporan "Digital 2024 Indonesia" mengindikasikan peningkatan yang signifikan dalam jumlah pengguna internet di Indonesia [1]. Data menunjukkan bahwa pada awal tahun 2024, jumlah pengguna internet di Indonesia mencapai 185,3 juta orang, yang setara dengan 66,5% dari total populasi Indonesia [1]. Meskipun internet memberikan banyak manfaat, penggunaan yang tidak tepat dapat menyebabkan dampak negatif pada kehidupan manusia. Salah satu dampak negatif ini adalah peningkatan kejahatan di dunia maya atau kejahatan siber [2]. Berdasarkan data yang diambil dari "Laporan Tahunan Layanan *Honeynet* BSSN 2023", total data statistik serangan yang berhasil ditangkap menggunakan *Honeypot* pada periode Januari sampai Desember 2023 sebanyak 603.276.807 kali serangan [3].

Penelitian ini bertujuan untuk menghadapi masalah keamanan jaringan yang berfokus pada serangan siber *Distributed Denial of Service (DDoS)* dan *SSH Brute force.* Serangan *DDoS* adalah tindakan kejahatan siber di mana aliran data tidak sah terus-menerus dikirimkan ke server atau sistem, menyebabkan kelebihan beban yang dapat menyebabkan penurunan kinerja atau kegagalan sistem, dengan tujuan mengganggu ketersediaan layanan sistem target dengan membuatnya tidak dapat diakses atau merespon permintaan [4]. Salah satu contoh kasus di Indonesia sempat terjadi serangan *DDoS* pada penyelenggaraan Pemilihan Umum 2024, tercatat sekitar ratusan juta akses ke domain-domain yang berkaitan dengan Pemilihan Umum 2024 yang mengakibatkan domain-domain tersebut tidak dapat diakses [5]. Serangan *brute force* pada protokol *Secure Shell (SSH)* adalah bentuk serangan siber yang bertujuan untuk mendapatkan akses tidak sah ke sebuah sistem. Serangan

ini dilakukan dengan cara mencoba berbagai kombinasi nama pengguna dan kata sandi secara otomatis hingga ditemukan kombinasi yang tepat untuk masuk ke sistem tersebut [6]. Pada rentang waktu Januari hingga Desember 2023, tercatat sekitar 11.081.392 upaya serangan *SSH Brute force* yang ditujukan ke situs-situs *web* yang terkait dengan pemerintahan di Indonesia. Serangan semacam ini menyebabkan dampak negatif yang signifikan, seperti penurunan kinerja sistem, risiko kebocoran data sensitif, dan potensi gangguan terhadap layanan-layanan publik yang dijalankan oleh entitas pemerintah. [3]. Keberadaan ancaman ini memicu kebutuhan akan solusi keamanan yang lebih efektif [7].

Dalam menghadapi tantangan ini, pengelolaan dan pengamanan jaringan menjadi penting, dimana penerapan *Intrusion Detection System (IDS)* sebagai sistem yang diterapkan untuk mendeteksi upaya-upaya penetrasi terhadap suatu sistem dengan mengawasi lalu lintas jaringan secara langsung [8]. *Software Defined Network (SDN)* juga digunakan sebagai alat kontrol terhadap infrastruktur jaringan secara terpusat [9]. Selain itu, penggunaan *Honeypot* juga penting sebagai alat pendeteksi serangan, tetapi juga sebagai alat untuk mempelajari taktik dan teknik peretas untuk meningkatkan kemampuan dalam menghadapi serangan siber [10]. Penerapan *Quality of Service (QoS)* memiliki peran penting dalam menghadapi serangan. Dengan menggunakan *QoS*, pemantauan dan analisis terhadap *throughput, latency, packet loss*, serta parameter *QoS* lainnya dapat dilakukan, memungkinkan evaluasi menyeluruh terhadap pengaruh serangan terhadap kualitas layanan jaringan [11].

Berdasarkan permasalahan diatas maka dibuat suatu rancangan topologi jaringan yang dapat di konfigurasi secara terpusat yang diharapkan dapat memberikan solusi dalam menghadapi serangan siber. Oleh karena itu, disusun penelitian ini pada skripsi yang berjudul "Analisis Sistem Keamanan Pada *Software-Defined Network* Dengan *Hybrid Honeypot* Menggunakan *Quality Of Service*".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, tantangan dalam penelitian yang dilakukan kali ini adalah sebagai berikut:

Dengan meningkatnya penggunaan internet, infrastruktur jaringan menjadi lebih rentan terhadap serangan siber. Ancaman yang semakin kompleks seperti *DDoS* dan *SSH Brute force* menunjukkan pentingnya menjaga keamanan sistem jaringan karena dampaknya yang luas dan signifikan. Serangan *DDoS* dapat membuat layanan *online* tidak dapat diakses, sementara serangan *SSH Brute Force* dapat mengakibatkan akses tidak sah ke sistem dan potensialnya mencuri data atau merusak konfigurasi. Dalam menghadapi tantangan ini, diperlukan upaya yang tidak hanya responsif terhadap serangan siber tetapi juga proaktif dalam melindungi infrastruktur. Oleh karena itu, penelitian ini bertujuan untuk merancang sistem jaringan yang dapat dikonfigurasi secara terpusat dengan memanfaatkan teknologi dan strategi keamanan seperti *IDS*, *SDN*, dan *Honeypot* untuk meningkatkan tingkat keamanan dan ketersediaan layanan dalam menghadapi serangan siber. Selain itu, penelitian ini juga akan menggunakan *Quality of Service (QoS)* sebagai parameter pengukuran kinerja layanan.

1.3 Pertanyaan Penelitian

Berdasarkan rumusan masalah diatas, maka pertanyaan peneliti dalam melakukan penelitian ini yaitu:

1. Bagaimana merancang sebuah sistem *Hybrid Honeypot* yang menggunakan *Intrusion Detection System (IDS)* sebagai mekanisme deteksi serangan, dan *Software-Defined Networking (SDN)* sebagai kontroler dalam arsitektur jaringan?
2. Bagaimana mengukur kinerja sistem *Hybrid Honeypot* yang menggunakan *Intrusion Detection System (IDS)* sebagai mekanisme deteksi serangan, dan *Software-Defined Networking (SDN)* sebagai kontroler dalam arsitektur jaringan?

1.4 Batasan Masalah

Berdasarkan rumusan masalah dan tujuan penelitian, maka untuk mewujudkan penelitian yang sesuai dengan masalah yang ada diperoleh batasan-batasan masalah penelitian sebagai berikut :

1. Penelitian ini dibatasi merancang *Software Defined Network* menggunakan *platform Floodlight*.
2. Penelitian ini dibatasi merancang *Software Defined Network* menggunakan *Open Virtual Switch*.
3. Penelitian ini dibatasi menerapkan *Intrusion Detection System (IDS)* menggunakan perangkat lunak *Snort*.
4. Penelitian ini dibatasi menerapkan *Hybrid Honeypot* menggunakan perangkat lunak *Dionaea* dan *Cowrie*.
5. Penelitian ini dibatasi pada analisis serangan *Distributed Denial of Service (DDoS) HTTP Flood, ICMP Flood, SYN Flood* dan serangan *SSH Brute Force.*
6. Penelitian ini dibatasi menggunakan perangkat lunak *Hping3* dan *Hydra* pada saat pengujian serangan.
7. Penelitian ini dibatasi pada manipulasi lalu lintas jaringan yang terjadi selama berlangsungnya serangan.
8. Penelitian ini dibatasi pada penggunaan parameter *Quality of Service* sebagai metode untuk mengukur performa jaringan.
9. Penelitian ini dibatasi pada pengukuran parameter *Quality of Service (QoS)* terhadap lalu lintas serangan pada perangkat *Honeypot*.

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah, dapat dijabarkan tujuan penelitian sebagai berikut:

1. Merancang sebuah sistem *Hybrid Honeypot* yang menggunakan *Intrusion Detection System (IDS)* sebagai mekanisme deteksi serangan, dan *Software-Defined Networking (SDN)* sebagai kontroler dalam arsitektur jaringan.

2. Mengukur kinerja sistem *Hybrid Honeypot* yang menggunakan *Intrusion Detection System (IDS)* sebagai mekanisme deteksi serangan, dan *Software-Defined Networking (SDN)* sebagai kontroler dalam arsitektur jaringan.

1.6 Manfaat Penelitian

Berdasarkan rumusan masalah, batasan masalah dan tujuan penelitian yang telah diuraikan diatas, maka dapat diketahui manfaat dari penelitian ini adalah:

1. Kegunaan Bagi Penulis
   a. Untuk dapat menerapkan ilmu yang diperoleh selama masa studi di perguruan tinggi.
   b. Untuk dapat memenuhi salah satu syarat dalam menyelesaikan kurikulum tingkat akhir Fakultas Informatika, Program Studi Teknik Informatika, Universitas Telkom Purwokerto.
   c. Untuk dapat merancang sebuah sistem *Hybrid Honeypot* yang menggunakan *Intrusion Detection System (IDS)* sebagai mekanisme deteksi serangan, dan *Software-Defined Networking (SDN)* sebagai kontroler dalam arsitektur jaringan.
2. Kegunaan Bagi Pembaca
   a. Memberikan wawasan cara merancang sistem terpusat dengan keamanan yang efektif mendeteksi dan merespons serangan.
   b. Menyediakan metodologi, implementasi dan evaluasi yang dapat dijadikan referensi bagi penelitian selanjutnya.
   c. Meningkatkan pemahaman tentang pentingnya keamanan jaringan dan berbagai teknik untuk melindungi infrastruktur IT.