BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG

Dengan kemajuan teknologi modern, internet menjadi sangat peting dalam segala aspek kehidpan manusia karena memudahkan komunikasi jarak jauh melalui jaringan dan juga sering digunakan sebaai media penyimpann data penting.[1] Internet juga menjadi kebutuhan yang tak terpisahkan dalam setiap aspek kehidupan manusia, memudahkan komuniksi jarak jauh melalui jaringa dan berperan sebagai media penyimpaan data penting.[2] Menurut data Badan Sibr dan Sandi Negara (BSSN), tercatat 190 juta percobaan serangan siber di Indonesia dari bulan januari hingga Agustus 2020. Angkaini meningkat signifikan dibandingkan dengan 39 juta kasus pada periode yang sama tahun sebelumnya, yang merupakan ancaman serius bagi pengguna internet di indonesia.[3]

Internet telah menciptakan sebuah dunia baru yang dikenal sebagai dunia maya. Ini adalah bentuk komunikasi berbantuan komputer yang menyediakan realitas virtual baru, yang bersifat tidak langsung dan tidak realistis.[4] Namun seringkali administrator server mengabaikan aspek keamanan yang diketahui rentan terhadap ancaman keamanan. Salah satu kekurangan yang diketahui rentan terhadap ancaman keamanan. Salah satu kekurangan yang sering muncul adalah ketidakpahaman administrator server terhadap efek samping dari aplikasi yang diinstall pada web server yang mereka Kelola. Pada dasarnya, Sebagian besar aplikasi ini diperlukan untuk memudahkan pekerjaan, namun Ketika aplikasi diinstal, hal tersebut membuka port atau port yang diperlukan untuk komunikasi dengan dunia luar. Port yang terbuka ini kemudian dapat menjadi jalan bagi malware untuk masuk dan menyusup kedalam sistem komputer.[5]

Serangan jaringan (hack) merupakan serangan yang dapat dilakukan pada

jaringan komputer yang terhubung ke Internet. Serangan ini dapat menyebabkan kesalahan atau malfungsi pada komputer atau server yang terkena dampaknya, yang pada gilirannya dapat berdampak signifikan pada sistem komputer atau server tersebut. Beberapa jenis serangan pada jaringan komputer atau server meliputi packet sniffing, spoofing, distributed denial of service (DDoS), DNS poison, Trojan horse, SQL injection, script kiddies, dan LAND attack. Ancaman serangan dapat dibagi menjadi dua kategori, yaitu serangan internal dan eksternal. Serangan internal dapat muncul ketika ancaman terjadi di dalam suatu organisasi dan dapat menyebabkan kerusakan pada organisasi itu sendiri atau ancaman yang dapat mengakibatkan kehilangan aset. Ancaman eksternal dapat muncul dalam bentuk serangan malware, pencurian data, akses tidak sah, dan penyalahgunaan sumber daya perusahaan. Kurangnya fungsionalitas dan konfigurasi jaringan dapat mengancam keamanan host dan membuka celah keamanan dalam sistem komputer Anda.[6]

Maka dari itu diperlukan perancangan sistem yang dapat mendeteksi dan memblokir serangan serangan *Distributed Denial Of Service* DDoS dan*man-in-the-middle* (MiTM).Oleh karena itu, diperlukan sistem keamanan jaringan yang aman dari serangan hacker. Ada beberapa metode dan alat yang tersedia untuk keamanan jaringan. Metode yang umum digunakan adalah IDS, yang memungkinkan IPS untuk memblokir serangan saat mendeteksi serangan.Ini dapat dilakukan dengan menggunakan metode "IDPS" untuk sistem deteksi dan pencegahan intrusi. Digunakan sebagai solusi untuk membantu administrator aplikasi sistem deteksi dan pencegahan intrusi IDPS memantau dan menganalisis paket berbahaya di jaringan.[8] Untuk dapat menyelesaikan masalah keamanan jaringan dengan mengintegrasikan IDPS *snort* dan *honeypots cowrie*. Penggunaan metode IDPS berfungsi untuk mendeteksi, mengidentifikasi, menganalisis dan mencegah ancaman menyerang sistem. Metode ini berfungsi sebagai firewall, mengizinkan dan memblokir. Ada beberapa jenis IPS, namun yang digunakan adalah sistem pencegahan intrusi berbasis jaringan “IDPS”. IDPS ini bekerja sejalan dengan perlindungan proaktif. Salah satunya adalahkeamanan open source (SNORT). Snort bertindak

seperti firewall yang dapat mengizinkan dan memblokir. Selain itu, Teknik yang digunakan untuk mendeteksi serangan mengunakan serangan berbasis tanda tangan.

Honeypots juga menjadi solusi pemantauan aktivitas penyerangan agar mengetahui bagaimana perilaku attacker untuk mendapatkan informasi. Honeypot adalah tools yang bertugas untuk mengelabui attacker agar membuat sistem terlihat persis seperti sistem aslinya. . Oleh karena itu, attacker menganggap intrusi sebagai sistem asli ketika diperintahkan untuk benar-benar menyerang server perangkap intrusi pada saat intrusi.

Sistem keamanan jaringan ini memiliki topologi star karena sistem dimonitor secara terpusat oleh administrator jaringan. Pusat Manajemen Jaringan sepenuhnya dikendalikan oleh perangkat router PC yang menyediakan akses ke *server web* dan layanan *server* DNS. Layanan ini dapat berjalan karena jalur protokol dan port dikendalikan sebagai firewall yang digunakan metode jaringan *zona demiliterisasi* (DMZ).

Untuk penelitian ini metode pengukuran yang digunakan adalah QOS (*Quality Of Service*) yang berfungsi mengontrol dan mengelola sumber daya jaringan dengan menetapkan prioritas untuk tipe data tertentu pada jaringan, dan untuk mengukur parameter-parameter dalam QOS yaitu Throughput,Delay,Jitter dan Paket Loss. Berdasarkan penelitian yang telah dilakukan sebelumnya penjelasan yang telah dipaparkan diatas, penelitian bermaksud untuk menganalisis dan merancang sebuah sistem keamanan jaringan dari kinerja DMZ,Snort dan *Honeypot cowrie* . Adapun analisis dan peracangan dalam penelitian ini mencakup mengenai permasalahan, Bagaimana kinerja tools snort dan honeypot cowrie menggunakan serangan *Distributed Denial Of Service* (DDoS) dan *Man in the Middle* dan mengetahui pengujian.

1.2 RUMUSAN MASALAH

Berdasarkan uraian diatas, permasalahan yang timbul diantaranya:

1. Bagaimana cara merancang suatu sistem keamanan jaringan menggunakan *DMZ, Snort IDPS* dan *Honeypot Cowrie*

2. Bagaimana kinerja tools snort IDPS dan honeypot menggunakan serangan *Distributed Denial Of Service* (DDoS) dan *Man in theMiddle*
3. Bagaiamana kinerja IDPS dengan *snort* dan *honeypot cowrie* berdasarkan parameter *Quality of Service* (QoS)?

1.3 PERTANYAAN PENELITIAN

Pertanyaan dari penelitian ini adalah:

1. Bagaiamana cara mensimulasikan sistem keamanan jaringan menggunakan IDPS dan *Honeypots* untuk keamanan jaringan
2. Bagaimana analisis simulasi sistem keamanan jaringan dalam menghadapi serangan dilakukan saat menguji serangan *Man in The Middle* (MiTM) dan DDOS

1.4 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1. Penerapan Honeypot Cowrie dan Snort *Intrusion Detection and Prevention Sytem* (IDPS)untuk mendeteksi serta memblokir serangan *Man in The Middle* (MiTM) dan *Distributed Denial Of Service* (DDoS)
2. Penggunaan tools snort dalam penerapan metode *Intrusion Detection and Prevention Sytem* (IDPS)
3. Parameter *Quality Of Service* untuk mengetahui kerja kinerja *Intrusion Detection and Prevention Sytem* (IDPS)
4. Perancangan jaringan menggunakan *Demilitarizes Zone* (DMZ) menggunakan tool *Iptables*

1.5 TUJUAN PENELITIAN

Berdasarkan latar belakang dan pertanyaan penelitian yang telah dibahas sebelumnya, tujuan dari penelitian ini adalah mensimulasikan sistem keamanan jaringan dengan menggunakan DMZ, Intrusion Detection Prevention System (IDPS) Snort honeypot cowrie yang dapat menganalisis dan mensimulasikan sistem ketika dilakukan pengujian dengan serangan DDoS dan MiTM dan menerapkan Quality of Service (QoS) dalam analisis serangan Distributed Denial

1.6 MANFAAT PENELITIAN

Adapun manfaat dari penelitian ini adalah:

1. Dapat merancang suatu sistem keamanan jaringan menggunakan *Snort* dan *Honeypot Cowrie.*
2. Dapat mengetahui kinerja tools *snort* dan *honeypot* menggunakan serangan *Distributed Denial Of Service* (DDoS) dan *Man in The Middle.*
3 Dapat Mengetahui kinerja IDPS *snort* dan *honeypot* berdasarkan parameter *Quality Of Service* (QOS)