BAB I

PENDAHULUAN

1.1 Latar Belakang

Ruangan KP yang terdapat pada departemen Bagian Layanan TI PT.Pusri Palembang memiliki jaringan komputer yang memfasilitasi layanan Jaringan bagi peserta kerja praktik dan karyawan, Namun saat ini jaringan pada Ruangan KP tersebut sering terjadi gangguan layanan atau *Downtime*, Hal ini akan mempengaruhi kinerja dari peserta kerja praktik dan karyawan yang terdapat pada Ruangan KP menjadi terganggu dan lambat di karenakan gangguan pada Jaringan Ini. Penyebab utama dari gangguan pada Jaringan ini yaitu Keamanan Jaringan yang belum optimal sehingga diperlukan peningkatan atau optimalisasi pada Jaringan, untuk mengantisipasi terjadinya penyalahgunaan jaringan oleh para hacker diperlukan peningkatan keamanan pada jaringan yang dibangun (Putra & Ramdhani, 2021). Maka dari itu peneliti berusaha untuk melakukan atau mencari solusi untuk optimalisasi keamanan jaringan pada Bagian Layanan TI tersebut.

Peneliti merencanakan solusi yang dapat meningkatkan keamanan pada jaringan yang sebelumnya pernah mengalami gangguan layanan dan mengantisipasi agar gangguan tersebut tidak terulang kembali yakni Peneliti akan melakukan penyelidikan terhadap penyebab gangguan jaringan tersebut yang di indikasikan akibat serangan *DdoS,* peneliti akan melakukan pengumpulan data pada jaringan dan sumber lainnya serta peneliti akan melakukan sebuah percobaan

pengujian dimana peneliti akan melakukan pengujian serangan lalu memantau, mengamati dan melakukan analysis ataupun yang disebut *Network Forensic*, *Network Forensic* adalah Cabang dari *Forensik* terkait dengan melakukan pemantauan, menganalisa lalu lintas jaringan komputer untuk mengumpulkan informasi, dan fungsinya meliputi semua kemungkinan yang dapat menyebabkan pelanggaran keamanan sistem(Surya Kusuma, 2023). Langkah *Network Forensic* yang akan Dilakukan Pada Jaringan dengan menggunakan *Tools Snort IDS* dan dengan Melakukan Beberapa pengujian Serangan Pada Jaringan, pengujian yang dilakukan yaitu pengujian serangan *DdoS* dan *Brute Force*, Peneliti mencoba Melakukan pengujian Serangan *Ddos* dan *Brute force* tersebut karena gangguan pada jaringan memiliki ciri-ciri yang sama dengan dampak serangan *Ddos* Dan *Brute force* yaitu Serangan nya dapat mengganggu layanan pada sebuah jaringan, Peneliti akan melakukan pengujian serangan dengan pengujian *Ddos* yang terdapat pada *Tools Pentmenu* dan *Brute force* Pada *Tools Ncrack*, Peneliti Juga akan melakukan skenario tambahan *Yaitu Port Scanning* pada jaringan karena *Port Scanning* merupakan langkah awal peretasan untuk menemukan *Port* yang terbuka pada jaringan untuk kemudian diserang hal ini dapat menyebabkan serangan *Ddos* dan *Brute force* dimulai karena Port yang dibiarkan terbuka.

Peneliti menemukan solusi terkait dengan masalah gangguan yang diketahui dengan ciri-ciri yang sama dengan serangan *Ddos* yaitu dengan melakukan optimalisasi keamanan pada jaringan dengan melakukan penerapan sebuah *Firewall* yang dapat memblock serangan dan Peneliti akan Menutup Port yang terbuka pada jaringan dengan memanfaatkan fitur yang ada pada Mikrotik sebagai

langkah optimalisasi. *Firewall* yang akan diterapkan pada jaringan yaitu *Firewall tarpit*, Peneliti memilih *Firewall tarpit* karena merupakan layanan pada sistem komputer yang disengaja memperlambat koneksi masuk ataupun suatu protocol yang akan membloking atau menghentikan serangan(Aulianita dkk., t.t.).

Berdasarkan uraian yang ada dimana peneliti akan mencoba melakukan sebuah Teknik *Network Forensic* pada jaringan karena berdasarkan permasalahan yang ada serangan tersebut memiliki ciri-ciri yang sama dengan serangan *Ddos* dan setelah diskusi yang dilakukan dengan administrator jaringan terkait peneliti mencoba menerapkan Teknik *Network Forensic* dengan melakukan pengujian serangan *Ddos* Dan *Brute force* pada Jaringan dan hasil pada proses tersebut peneliti untuk meng-optimalkan Jaringan tersebut akan menerapkan *Firewall* yang efektif untuk memblokir terhadap serangan tersebut yaitu *Firewall tarpit* maka dari Itu peneliti mengangkat topik penelitian berjudul "**Implementasi *Firewall tarpit* Untuk Optimalisasi Keamanan Jaringan Bagian Layanan TI PT.Pusri Palembang Metode NSIT SP 800-86** ".

1.2 Rumusan Masalah

Dari latar belakang yang telah dikemukakan diatas, maka rumusan masalah dari penelitian ini adalah bagaimana cara mengoptimalkan keamanan pada jaringan terhadap masalah gangguan layanan jaringan atau *downtime* dengan indikasi Serangan *DdoS* pada jaringan di Bagian layanan TI PT.Pusri Palembang.

1.3 Batasan Masalah

Adapun Batasan Masalah dari Penelitian Ini yang peneliti Ambil yaitu Sebagai Berikut:

1. Optimalisasi Keamanan Jaringan Ruangan KP dengan Menerapkan *Firewall tarpit* sebagai keamanan jaringan
2. Pengujian Serangan yang dilakukan adalah *Ddos* dan *Brute force*.
3. *Tools* yang dipakai pada pengujian yaitu *Pentmenu* dan *Ncrack*

1.4 Tujuan Penelitian

Berdasarkan Judul yang dikemukakan, maka tujuan dari penelitian ini adalah "Melakukan optimalisasi keamanan pada Jaringan dengan penerapan *Firewall tarpit* untuk mencegah dari serangan *Ddos* dan *Brute force* pada Departemen bagian Layanan TI PT.Pusri Palembang".

1.5 Manfaat Penelitian

Manfaat Yang akan Diperoleh Dari Hasil penelitian ini meliputi Berbagai Manfaat, Yaitu Sebagai Berikut.

a. Bagi penulis

   Memperdalam wawasan terhadap bidang *Network Forensics* dan keamanan jaringan komputer serta dapat mengembangkan keterampilan teknis dalam melakukan analisis keamanan dan penerapan keamanan pada jaringan serta pengujian keamanan.

b. Bagi Instansi perusahaan

Agar dapat Lebih Meningkatkan Keamanan jaringan terutama dari Serangan *Ddos* dan *Brute force.*

c. Bagi akademik

Sebagai Panduan bagi peneliti selanjutnya yang berkaitan dengan *Network Forensics.*

1.6 Penelitian Terdahulu

Adapun penelitian terdahulu sebagai penulis gunakan sebagai referensi untuk penelitian ini adalah sebagai berikut :

1) Penelitian yang dilakukan oleh Mustazzihim Suhaidi, Nurhadi yang mana pada penelitian ini, penulis mengimplementasikan dan melakukan analisis Terhadap keamanan jaringan pada STIA Lancang Kuning Dumai di Kota Dumai, dimana Tujuan utama dari penelitian ini adalah untuk mengidentifikasi celah keamanan dalam jaringan dan melindungi sistem dari ancaman yang mungkin timbul, pada penelitian ini metode yang digunakan yaitu Metode *SDLC,* Hasil dari penelitian ini, Penulis berhasil meningkatkan keamanan jaringan mereka dan mengurangi resiko terhadap serangan dan pencurian data (Suhaidi & Nurhadi, 2023).

2) Penelitian yang dilakukan oleh Sri Suharti, Anton Yudhana, Imam Riadi yang mana pada penelitian ini, Penulis melakukan forensik jaringan, *Denial Distributed of Service* pada sistem operasi *proprietary* Windows dan mengimplementasikan *firewall network layer* untuk menghentikan serangan *Ddos* pada jaringan berbasis lokal dan luas, pada penelitian ini metode

menggunakan tahapan *Analyze ,Design,Develop,Implement and Evaluate (* ADDIE) dan perancangan desain *Host-Based Intrusion Detection System (*HIDS*),* Hasil dari penelitian ini, Memberikan nilai akurasi tool *Ddos Slowloris* yang bekerja pada tool *Ddos* yang paling merusak dengan keakurasian peningkatan trafik sebesar 92,84%, penurunan performa server sebesar 78% yang mengakibatkan *server down* dibandingkan dengan LOIC UDP, LOIC TCP dan PoD. Pada *slowloris* membutuhkan paket data yang sedikit dibandingkan *LOIC UDP* dan yang lainnya dalam melakukan serangan , hal ini membuat serangan tidak mudah diketahui sehingga harus menerapkan *HIDS* untuk peringatan sebuah serangan, peringatan terbanyak oleh HIDS Snort terdeteksi pada *Ddos,* Berdasarkan hal Tersebut maka untuk menghentikan *Ddos* Dengan *Firewall* pada layer network dengan keefektifan rata-rata sebesar 98.91% (Suharti et al., 2022).

3) Penelitian yang dilakukan oleh Ahmad Sakhowi Amin dan Pipit Dewi Arnesia yang mana penelitian ini, penulis melakukan pengembangan sistem keamanan jaringan Menggunakan *Network Forensics* dimana dilaksanakan untuk menguji dan menganalisis agar memperoleh data serangan dan ancaman, pada penelitian ini metode yang dipakai yaitu *Network Forensics,* Hasil dari penelitian ini yaitu Sistem jaringan yang sedang berjalan dilakukan pengujian dan analisis dengan target beberapa port , *Network forensics* yang dikembangkan dalam penelitian ini mampu mendeteksi dan memblokir saat terjadi penyerangan atau penyusupan(Amin & Arnesia, 2023)

4) Penelitian yang dilakukan oleh Abdul Khaliq dan Sri Novida Sari yang mana penelitian ini, penulis melakukan pemanfaatan kerangka kerja Forensik Jaringan untuk identifikasi serangan dengan menggunakan sistem deteksi intrusi (IDS), Pada penelitian ini menggunakan metode IDS Sebagai deteksi serangan dengan tujuan untuk mengimplementasikan IDS pada sistem jaringan dan menganalisis log IDS untuk menentukan jenis dan serangan jaringan komputer dan metode penelitian yang dipakai adalah metode terapan, hasil dari penelitian Ini adalah IDS efektif dalam mendeteksi aktivitas pemindaian jaringan dan serangan *Ddos*, IDS memberikan peringatan kepada administrator karena ada aktivitas yang melanggar aturan di IDS(Penelitian et al., 2022).

5) Penelitian yang dilakukan oleh Firmansyah, Abdul Fadlil dan Rusydi Umar yang mana pada penelitian ini, penulis melakukan Identifikasi Bukti Forensik jaringan virtual Router dengan menggunakan Metode *NSIT SP800-86,* Pemanfaatan metode *National Institute of standard and Technology (NSIT)* yang meliputi, Koleksi, Pemeriksaan,analisis dan pelaporan dapat diulang dan dipertahankan dengan data yang sama, Berdasarkan hasil dari pengujian Forensik, penggunaan metode NSIT pada Sistem Forensik yang telah dibangun dengan objek Virtual router, dapat digunakan investigator sebagai identifikasi bukti serangan siber.(Yasin dkk., 2021a).