BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan adalah hal yang sangat penting di era sekarang, terlebih lagi pada jaringan didalam sebuah organisasi atau institusi yang dimana terdapat sebuah informasi dan data yang harus di amankan.

Data dan informasi adalah hal yang vital untuk diamankan dari ancaman, serangan, dan pencurian. Semakin besar sebuah institusi maka semakin banyak data dan informasi yang harus diamankan.

Data dan informasi pada umumnya disimpan dalam sebuah *server* yang diletakkan didalam jaringan *internal* . Untuk mengamankan data dan informasi tersebut, dibutuhkan sebuah *firewall* serta pemisah antara jaringan *internal* dan *server*.

Dalam keamanan komputer, *Demilitarized Zone* (DMZ) merupakan suatu area didalam sebuah jaringan dimana seorang *user* akan dimasukkan kedalam area jaringan netral diantara sebuah jaringan publik dan jaringan *internal* atau privat. Pembentukan area *Demilitarized Zone* (DMZ) ini dilakukan untuk menghalangi akses jaringan internal suatu organisasi atau perusahaan yang berisi data-data dan informasi penting dari pihak yang tidak berkepentingan. [1]

Istilah *Demilitarized Zone* (DMZ) ini pertama kali digunakan pada zona penyangga yang dibuat untuk wilayah perbatasan Korea Utara dan Korea Selatan yang mengikuti ketentuan PBB pada tahun 1950. [1]

Menurut Wangchuk (2018) penggunaan perangkat lunak *Graphical Network Simulator 3* (GNS3) dapat dilakukan untuk mensimulasikan sebuah jaringan, meniru sebuah jaringan dan menjalankan perangkat-perangkat untuk dipelajari para *administrator* jaringan guna meningkatkan keterampilan dan pengetahuan. Dalam penelitian tersebut 67,6% responden setuju bahwa aplikasi GNS3 mudah digunakan untuk keperluan pembelajaran dan sebanyak 50,30% responden merasa bahwa konsep administrasi dan jaringan yang ada pada aplikasi GNS3 di jaringan virtual bisa dilakukan dengan mudah dan sangat mudah untuk di pahami. [2]

Berdasarkan uraian di atas, maka penulis membuat penelitian dengan judul "ANALISIS DAN IMPLEMENTASI *DEMILITARIZED ZONE* (DMZ) UNTUK MENINGKATKAN KEAMANAN JARINGAN PADA MIKROTIK MENGGUNAKAN GNS3". Pada penelitian ini, penulis bertujuan untuk membuat simulasi pada aplikasi GNS3 dan menerapkan *Demilitarized Zone* (DMZ) dengan menggunakan perangkat Mikrotik sebagai *router* dan *firewall* karena perangkat router Mikrotik mempunyai fitur yang cukup lengkap. Selain itu, penulis juga menggunakan *Intrusion Detection System* Suricata sebagai *monitoring log* karena bersifat *open source*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, permasalahan yang penulis dapat rumuskan adalah :

1. Bagaimana mengimplementasikan simulasi jaringan sistem *Demilitarized Zone* (DMZ) pada aplikasi GNS3 untuk mengamankan sebuah jaringan lokal menggunakan perangkat Mikrotik ?
2. Bagaimana hasil perbandingan analisis sebelum dan sesudah diterapkannya firewall di perangkat mikrotik pada area DMZ dan jaringan Internal terhadap serangan *Intruder* ?

1.3 Batasan Masalah

Batasan masalah diperlukan untuk mengarahkan pekerjaan dan pembahasan proyek penelitian agar tetap dalam ruang lingkup sesuai topik penelitian. Batasan masalah yang digunakan dalam penelitian ini adalah :

1. Sistem keamanan jaringan *Demilitarized Zone* (DMZ) dilakukan dengan melakukan simulasi jaringan menggunakan aplikasi GNS3.
2. Analisis dibatasi pada infrastruktur jaringan, topologi jaringan, dan hak akses pengguna dari jaringan internal atau *untrusted network*.
3. Infrastruktur dan topologi jaringan yang diteliti merupakan sebuah rancangan jaringan lokal yang penulis buat.
4. Analisis sistem keamanan jaringan dilakukan dengan menggunakan IDS Suricata sebagai *log monitoring*.
5. Penelitian ini memanfaatkan perangkat Mikrotik sebagai *router* dan *firewall*.

1.4 Maksud dan Tujuan Penelitian

Berdasarkan judul penelitian, ada beberapa maksud dan tujuan penelitian ini, yaitu :

1. Untuk merancang dan membangun sistem keamanan jaringan berbasis *Demilitarized Zone* (DMZ) menggunakan aplikasi simulasi GNS3.
2. Pemanfaatan perangkat *router* Mikrotik dan *Intrusion Detection System* (IDS) Suricata sebagai penunjang sistem keamanan jaringan berbasis *Demilitarized Zone* (DMZ) untuk sebuah server dan jaringan lokal.

1.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan akan memberi manfaat sebagai berikut :

1. Bagi penulis
   a. Dapat mengetahui bagaimana proses perancangan sistem keamanan jaringan lokal berbasis *Demilitarized Zone* (DMZ) .
   b. Dapat mengetahui bagaimana cara mengamankan server dan jaringan lokal dengan perangkat mikrotik.
   c. Dapat mengetahui bagaimana cara mendeteksi sebuah serangan menggunakan IDS Suricata.
   d. Dapat mengetahui bagaimana membangun sebuah simulasi jaringan berbasis *virtual device* menggunakan aplikasi GNS3.
2. Bagi pembaca
   a) Dapat mempelajari bagaimana membangun simulasi jaringan dengan menggunakan aplikasi GNS3.
   b) Dapat mempelajari bagaimana proses dari keamanan jaringan berbasis DMZ menggunakan *router* mikrotik.

c) Dapat mempelajari bagaimana proses deteksi serangan menggunakan IDS Suricata.

d) Dapat menjadikan referensi pembelajaran atau penelitian mengenai sistem keamanan jaringan berbasis *Demilitarized Zone* (DMZ).

1.6 Metode Penelitian

Ada beberapa metode yang digunakan dalam penelitian ini dan akan dijabarkan pada sub bab berikut ini.

1.6.1 Metode Pengumpulan Data

Dalam penelitian ini, penulis menggunakan beberapa metode penelitian yang berhubungan dengan pokok permasalahan diantaranya :

1. Metode Studi Literatur

   Pada metode ini, penulis mengambil data dari berbagai sumber sebagai referensi yang bersumber dari buku-buku, jurnal, dan e-book yang berkaitan dengan penelitian yang sedang dijalankan.

2. Metode Analisis

   Di metode ini penulis melakukan analisis sistem yang sedang dijalankan, analisis keamanan sistem dan analisis kebutuhan sistem serta kebutuhan pengguna.

1.6.2 Metode Perancangan Jaringan PPDIOO

PPDIOO merupakan metode analisis sampai pengembangan instalasi jaringan komputer yang dikembangkan oleh Cisco pada materi *Designing for Cisco Internetwork Solution* (DESGN) yang mendefinisikan secara terus

menerus siklus hidup layanan yang dibutuhkan untuk pengembangan jaringan komputer atau teknologi terkait. [3]

Ada beberapa tahapan pada metode analisis PPDIOO ini yaitu :

1. *Prepare* (persiapan)

   Fase *prepare* (persiapan) yaitu menetapkan kebutuhan organisasi dan bisnis dengan dilakukannya analisa pada jaringan komputer yang sedang berjalan, mengembangkan strategi jaringan berdasarkan hasil dari analisis jaringan komputer yang sedang berjalan, dan mengusulkan konsep arsitektur dengan level tingkat tinggi.

2. *Plan* (Perencanaan)

   Pada fase perencanaan ini persyaratan jaringan berdasarkan kebutuhan jaringan, fasilitas, dan tujuan diidentifikasi. Pada fase ini juga detail karakteristik dari jaringan, perbandingan kinerja potensial dan aktual di deskripsikan.

3. *Design* (Desain)

   Fase desain atau perancangan ini memiliki persyaratan bisnis dan teknis berdasarkan kondisi sebelumnya yang dapat digunakan untuk mengembangkan desain jaringan di dalam fase ini. Pemetaan topologi dan arsitektur jaringan yang akan digunakan akan dirancang sehingga dapat menjelaskan implementasi dari rangkaian sistem jaringan.

4. *Implement* (Implementasi)

Pada fase *implement* ini akan dilakukan instalasi pada perangkat-perangkat penunjang dan dikonfigurasi sesuai spesifikasi desain.

5. *Operate* (Operasi)

Pada fase operasi, pengamatan dan pemeliharaan dilakukan terhadap sistem jaringan yang sudah terpasang sehingga dapat berjalan dengan baik dan melakukan perbaikan jika ditemukan kerusakan pada perangkat.

6. *Optimize* (Optimasi)

Fase terakhir yaitu optimasi. Pada fase ini, kesadaran proaktif seorang manajer jaringan dilibatkan untuk mengidentifikasi dan menyelesaikan masalah sebelum persoalan tersebut mempengaruhi jaringan.

Model metode PPDIOO yang telah dijabarkan dapat dilihat pada gambar 1.1.

Gambar 1. 1 Metode Analisis PPDIOO

1.6.3 Metode Monitoring

Dalam metode ini penulis melakukan monitoring terhadap sistem keamanan yang diimplementasikan menggunakan Suricata sebagai *free open source Intrusion Detection System*(IDS) serta mengamati langsung dari perangkat-perangkat yang digunakan selama penelitian.

1.7 Sistematika Penulisan

Penulisan skripsi ini dibagi menjadi lima bab yang memiliki sub-bab pokok pembahasan dan satu daftar pustaka. Adapun sistematika penulisan skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Berisi tentang tinjauan pustaka, dasar-dasar teori yang digunakan dalam penyusunan skripsi yang diambil dari berbagai sumber

seperti jurnal, buku, literatur dan artikel dari *website* resmi yang ada di internet.

BAB III METODE PENELITIAN

Berisi tentang analisis sistem yang akan dibangun, perancangan dan gambaran umum system, serta analisis kebutuhan sistem dan perancangan topologi jaringan berbasis *Demilitarized Zone* (DMZ).

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini memaparkan hasil dari tahapan penelitian mulai dari analisis dan konfigurasi setiap perangkat, implementasi desain, serta uji keamanan sistem *firewall* berbasis *Demilitarized Zone* (DMZ).

BAB V PENUTUP

Pada bab terakhir ini berisi kesimpulan dan saran dari penulis yang dirangkum setelah melalui proses penelitian.