BAB I PENDAHULUAN

I.1 Latar Belakang

Teknologi informasi telah berkembang pesat sejak komputer pertama diciptakan. Seiring dengan perkembangan bidang ini, pengolahan dan penyetoran data menjadi salah satu poin terpenting yang perlu diperhatikan pengguna. Metode pengolahan yang baik dapat menghasilkan informasi bermanfaat.

Dengan kemajuan dalam bidang jaringan komputer, informasi dapat diperoleh dengan mudah. Secara khusus, data dan informasi dapat ditemukan di *World Wide Web* berkat teknologi internet. Di zaman sekarang ini, mengirim data secara *online* dapat tercapai dengan mudah dan nyaman.

Tetapi, hal yang patut diperhatikan dalam zaman yang berputar di sekitar teknologi ini adalah keamanan data. Dengan lahirnya internet, siapa saja dapat melihat data-data sebuah perusahaan, bahkan data-data yang konfidensial. Seorang penyerang (*attacker*) dapat mendapatkan data dan informasi rahasia jika data dan informasi tersebut tidak diamankan dengan baik.

Jika suatu organisasi mempunyai sistem jaringan tersendiri, seorang yang sudah mempunyai akses kedalam sistem jaringan, atau dapat disebut *insider*, dapat menyalahgunakan akses mereka untuk melakukan hal yang dapat melakukan kerusakan, baik secara sengaja maupun tidak sengaja. *Insider* tersebut ini juga dapat mengakses perangkat-perangkat lain dalam jaringan tersebut jika tidak ada proteksi yang diimplementasikan. Peristiwa ini dinamakan *insider attack* (Bellovin, 2008).

Dikarenakan seorang *insider* sudah mendapatkan izin untuk memakai sistem internal jaringan, *insider* tersebut tidak perlu meretas *firewall* eksternal sistem, dan dapat dengan mudah meretas perangkat-perangkat yang ada di dalam sistem. Adapun beberapa tujuan dari *insider attack* adalah *insider fraud*, sabotase, dan pencurian data (Saxena et al., 2020). Pada *CSI/FBI (Computer Security Institute, Federal Bureau of Investigaion) Computer Crime and Security Survey* yang diadakan pada 2003 ditemukan bahwa 56% dari responden survey melaporkan penggunaan sistem komputer yang tidak sah dalam 12 bulan terakhir. Dari semua

tipe penyerangan yang dilaporkan, pencurian data dilaporkan dalam 22% laporan, akses *insider* dengan 45%, dan penyalahgunaan jaringan *insider* dengan 80% kasus, dengan total kerusakan berestimasi $84 miliar USD. (Almann & Kelly, 2008)

Salah satu metode untuk mengamankan data dari *insider attack* adalah dengan pendekatan jaringan yang dinamakan *Microsegmentation*. Organisasi umumnya menerapkan keamanan hanya untuk elemen perusak dari luar sistem yang ingin masuk ke sistem. Jika elemen perusak tersebut sudah didalam sistem, tidak ada sarana untuk memberhentikan elemen tersebut. *Microsegmentation* berusaha menangani hal tersebut dengan mengisolasi setiap bagian internal dalam sebuah jaringan sistem. Dengan ini, elemen perusak yang masuk ke dalam sistem tidak dapat melakukan hal-hal merugikan yang berkaitan dengan bagian internal yang terisolasi. (Huang et al., 2019)

Untuk memaksimalkan keamanan lebih lanjut, *Microsegmentation* juga dapat digabungkan dengan *Next-Generation Firewall*. *Next-Generation Firewall* dapat memindai lebih banyak informasi dari paket data dibanding dengan *Firewall* tradisional, dengan fitur-fitur seperti *Deep Packet Inspection*. *Next-Generation Firewall* juga dapat menganalisa paket-paket data yang dikirim dari suatu perangkat di suatu segmen ke perangkat ke segmen yang sama, berbeda dengan *Firewall* tradisional yang hanya dapat menganalisa paket yang masuk/keluar dari sebuah jaringan (Miller, 2011).

Setelah meneliti permasalahan terhadap sistem jaringan dengan metode *insider attack*, salah satu hal yang optimal untuk dilakukan adalah memperkuat bagian internal jaringan agar data-data yang ada dapat disimpan dengan aman. Hal ini dapat dilakukan dengan mengimplementasikan *microsegmentation* dalam sistem, serta juga mengimplementasikan *Next-Generation Firewall* untuk mengamankan sistem jaringan lebih lanjut. Dalam penelitian ini, akan disimulasikan seorang *insider* melakukan *distributed denial of service* terhadap server internal sebagai sebuah bentuk dari *insider attack*, yang lalu akan diamati dampak serangannya. Setelah itu, akan diimplementasikan kombinasi *microsegmentation* dan *Next Generation Firewall* untuk memperketat bagian internal sistem jaringan tersebut, dan akan disimulasikan lagi serangan setelah *microsegmentation* dan *Next-*

Generation Firewall telah diimplementasikan. Lalu, akan dicatat lagi hasil dari serangan tersebut. Hasil akhir penelitian ini adalah perbandingan dampak dari kedua serangan tersebut, dan dampak dari pengimplementasian *microsegmentation* beserta *Next-Generation Firewall* pada sebuah sistem jaringan.

I.2 Rumusan Masalah

Rumusan masalah untuk penelitian ini adalah sebagai berikut:

1. Bagaimana cara merancang dan mengimplementasikan *microsegmentation* dengan *Next-Generation Firewall*?
2. Bagaimana dampak *microsegmentation* untuk memitigasi DDoS dan *insider attack* dalam sebuah sistem jaringan?
3. Bagaimana *microsegmentation* mempengaruhi kualitas jaringan?
4. Bagaimana *microsegmentation* mempengaruhi sumber daya sistem?

I.3 Tujuan Penelitian

Tujuan untuk penelitian ini adalah sebagai berikut:

1. Melakukan perancangan dan mengimplementasikan *microsegmentation* dengan *Next-Generation Firewall*.
2. Mengukur dampak *microsegmentation* dan *Next-Generation Firewall* dalam memitigasi serangan DDoS dan *insider attack.*
3. Mengukur dampak *microsegmentation* dan *Next-Generation Firewall* terhadap kualitas jaringan.
4. Mengukur dampak *microsegmentation* dan *Next-Generation Firewall* terhadap sumber daya sistem.

I.4 Batasan Penelitian

Agar penelitian terfokus pada satu bidang dan tidak meluas dari bidang yang dimaksud, ada beberapa batasan penelitian yang akan diterapkan:

1. Penelitian ini menggunakan pendekatan *lifecycle* PPDIOO sampai dengan tahap *Design*.
2. Metrik jaringan yang akan dilakukan *logging* adalah *one-way delay, IP Packet Delay Variation*, *Packet Loss*, dan *Capacity.*

3. Metrik sumber daya yang akan dilakukan *logging* adalah CPU dan *memory utilization* untuk *server* dan *firewall*.

I.5 Manfaat Penelitian

Manfaat dari Penelitian ini diantaranya:

1. Manfaat teoritis, sebagai penelitian untuk mengetahui dampak mikrosegmentasi terhadap sisi fungsionalitas, keamanan, kualitas jaringan, dan pemakaian sumber daya, serta mengukur besar dampak tersebut dengan jaringan tanpa mikrosegmentasi.
2. Manfaat praktis, sebagai referensi untuk mengimplementasi mikrosegmentasi untuk mengamankan data, server, atau *host* dalam sebuah jaringan.

I.6 Sistematika Penulisan

Sistematika penulisan penelitian ini diuraikan sebagai berikut:

Bab I Pendahuluan

Bab ini membahas latar belakang penelitian, rumusan serta batasan masalah pada penelitian, tujuan penelitian, manfaat penelitian, serta sistematika penulisan laporan penelitian.

Bab II Tinjauan Pustaka

Bab ini berisi penjelasan dari beberapa teori, teknologi, dan metode yang akan digunakan dalam pengerjaan penelitian.

Bab III Metodologi Penelitian

Bab ini berisi penjelasan tentang metodologi yang akan dipakai, dan bagaimana metodologi tersebut dipakai dalam penelitian ini.