BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring dengan berkembangnya teknologi digital yang dapat digunakan secara luas oleh masyarakat sekarang ini, banyak perubahan yang terjadi pada kehidupan sehari – hari. Perubahan itu diantaranya terjadi di bidang transaksi data yang dilakukan oleh banyak pihak melalui jaringan internet. Transaksi data yang terjadi pada masa ini meliputi banyak data sensitif yang dikirimkan melalui internet. Hal ini memungkinkan terjadinya kejahatan baru, yaitu pencurian data yang dikirimkan melalui internet. Hal ini dapat terjadi pada siapapun, baik terhadap pihak individu, kelompok, maupun kepada pihak perusahaan berskala global, seperti yang baru – baru ini terjadi terhadap Facebook. Pada kejadian tersebut, ratusan ribu data akun pengguna Facebook diretas. Akibatnya, data pribadi dari akun pengguna Facebook diambil tanpa izin oleh pihak Cambridge Analytica. Data – data yang dicuri dari Facebook tersebut meliputi beberapa hal termasuk ke dalam privasi, seperti nama, jenis kelamin, asal, nomor telpon, dan alamat tempat tinggal [1].

Pencurian data yang terjadi pada Facebook membuktikan bahwa pencurian data tidak memandang siapa pun dalam kejahatan tersebut. Pencurian data dapat terjadi pada siapa pun, baik pihak yang diserang menyadarinya atau tidak. Jika disadari, pihak yang diserang akan dapat melakukan pencegahan saat data tersebut sedang diambil atau diunduh oleh pihak penyerang. Tetapi pada sebagian besar kasus, pihak yang diserang tidak pernah menyadari bahwa dirinya sedang menjadi target dari pencurian data. Kasus tersebut juga menunjukan, bahwa pencurian data dapat terjadi kapanpun. Untuk itu, diperlukan sebuah sistem keamanan yang dapat melindungi data yang sedang dikirimkan, untuk memperlambat terjadinya pencurian data. Sistem keamanan

ideal tersebut berupa sistem keamanan yang dapat mengenkripsi atau mengautentikasi data yang dikirimkan, sehingga pihak yang tidak ditujukan untuk dikirim data tersebut tidak dapat mengaksesnya, karena tidak memiliki kunci untuk dekripsi atau autentikasinya.

Berdasarkan hasil penelitian yang pernah dilakukan[2] tentang efek penggunaan Virtual Private Network (VPN) pada sebuah jaringan, paket data yang dikirimkan melalui jaringan tersebut tidak terlalu banyak terpengaruh oleh serangan *blackhole* dan *rushing*. Hasil dari penelitian tersebut menunjukan nilai Quality of Service (QoS) dari jaringan tersebut. Didapat nilai *throughput* 1253.16 Kbps, *delay* 394.17 ms, dan *packet loss* 9.22% dari jaringan yang diberi tambahan keamanan dan diuji dengan serangan *blackhole*. Hasil tersebut lebih baik dibandingkan dengan jaringan yang tidak diberi keamanan tambahan. Sedangkan untuk serangan *rushing* terhadap jaringan tanpa keamanan tambahan didapat hasil QoS *throughput* 740.76 Kbps, *delay* 233.53 ms, dan *packet loss* 2.2%. Hasil ini lebih buruk dibandingkan dengan jaringan yang diberi keamanan tambahan.

Untuk itu, pada penelitian ini penulis mensimulasikan sistem keamanan tersebut terhadap serangan Denial of Service (DOS) dan *Packet Sniffing* dan kemudian mengukur performansi dari jaringan tersebut. Performansi jaringan yang akan diukur adalah *throughput*, *delay*, dan *packet loss* dari sistem yang dilengkapi dengan sistem keamanan tambahan dan tidak.

1.2 Tujuan

1. Mengamati dan menganalisis performansi jaringan Internet Protocol (IP) dengan dan tanpa VPN.
2. Melakukan simulasi serangan terhadap jaringan tersebut untuk kemudian diukur kembali performansinya

1.3 Rumusan Masalah

Sistem jaringan IPv4 memiliki masalah pada sisi keamanannya dibandingkan dengan IPv6. IPv4 tidak memiliki keamanan sedikitpun, sedangkan IPv6 memiliki keamanan tambahan dalam bentuk Authentication

Header dan Encrypted Security Payload. Maka dari itu, bagi pelanggan yang menggunakan IPv4 sebagai sistem jaringan utamanya akan rentan terhadap serangan.

Sistem keamanan yang digunakan pada penilitian ini adalah VPN *tunnel mode* dimana sistem keamanan tersebut akan menyembunyikan seluruh *Internet Protocol Address* (IP Address) dan memberikan IP Address baru. VPN *tunnel mode* digunakan karena memberikan proteksi lebih jika dibandingkan dengan VPN *transport mode*.

1.4 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Tipe IP yang digunakan adalah IPv4 agar dapat diberikan perlindungan tambahan
2. Sistem keamanan yang digunakan adalah VPN tunnel mode untuk melindungi seluruh paket IP yang dikirimkan.
3. Jenis serangan yang digunakan adalah Mac Overflow dan DoS untuk melumpuhkan PC target.
4. Parameter performansi yang diukur adalah throughput, delay, dan packet loss sebagai acuan utama performansi jaringan.

1.5 Metode Penelitian

Penelitian dilakukan dengan menggunakan simulasi. Simulasi pertama yaitu melakukan pengujian performansi pada jaringan IPv4 untuk dijadikan sebagai landasan performansi dari jaringan tersebut. Simulasi kedua yaitu memberikan keamanan tambahan pada jaringan tersebut dengan menggunakan VPN tunnel mode, kemudian diukur kembali performansi dari jaringan tersebut. Simulasi ketiga melakukan serangan terhadap jaringan yang tidak menggunakan keamanan tambahan dan mengukur performansinya. Simulasi keempat melakukan serangan terhadap sistem yang diberikan keamanan tambahan dan mengukur performansinya.

1.6 Manfaat Penelitian

Hasil dari penelitian ini diharapkan akan memberikan data yang cukup sebagai pertimbangan untuk pemasangan keamanan tambahan kepada jaringan yang masih menggunakan IPv4.

1.7 Sistematika Penulisan

Pada penelitian ini terbagi menjadi lima bagian dengan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang, tujuan, rumusan dan batasan masalah, dan metode yang digunakan pada penelitian ini.

BAB II DASAR TEORI

Bab ini membahas tentang teori – teori yang digunakan dalam penelitian ini, yakni IP, *Intenet Protocol Security* (IPSec), VPN, *throughput*, *delay*, dan *packet loss.*

BAB III PERANCANGAN SIMULASI

Bab ini membahas alur pengerjaan penelitian yang dilakukan, serta skenario penelitian yang dilakukan.

BAB IV ANALISIS HASIL SIMULASI

Bab ini berisi tentang simulasi jaringan dan hasil dari setiap simulasi berdasarkan parameter yang telah ditentukan.

BAB V PENUTUP

Bab ini berisi kesimpulan dari bab – bab yang telah dituliskan sebelumnya dan saran untuk pengembangan selanjutnya.