BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini perkembangan dan pertumbuhan teknologi pada bidang komunikasi serta informasi mengalami peningkatan yang pesat, salah satu dampak dari kemajuan ini terlihat didalam sistem pengolahan data. Dengan memakai media telekomunikasi data akan dikirim dari satu lokasi ke lokasi lainya. Proses transfer data dilakukan melalui media transmisi elektronik, media tersebut dikenal dengan sebutan komunikasi data (*data communication*). Penggunaan komunikasi data biasanya dilakukan ketika akan menjalankan pertukaran data pada jaringan komputer, kata jaringan digunakan jika ditemukan minimal dua atau lebih perangkat yang terkoneksi satu dengan yang lain. Untuk menjalankan kegiatan tersebut diperlukan sebuah *protocol* yang bisa menjalankan kegiatan pertukaran data, Maka dari itu dipakailah *protocol* yang mendefinisikan bagaimana data dipertukarkan, dan *File Transfer Protocol* (FTP) merupakan salah satu *protocol* yang sering dipakai.

Pada dasarnya *File Transfer Protocol* (FTP) sebagai *protocol* yang mempunyai tugas sebagai media transfer data atau file dalam lingkup suatu jaringan (*network*) yang belandaskan koneksi *Transmission Control Protocol* (TCP). Penggunaan *protocol* FTP menjadi salah satu pilihan yang tepat dalam penyimpanan file, karena proses *upload* dan *download* dari komputer *server* ke *client* ataupun sebaliknya bisa digunakan secara efisien [1]. FTP menjadi teknik pilihan yang tepat untuk menyimpan dengan kecepatan mentransfer file yang cukup baik, namun dengan perkembangan teknologi yang pesat ini banyak tools yang dapat digunakan untuk melakukan tindakan kejahatan seperti *bruteforce* FTP, *port scanning*, dan *Internet Control Message protocol Flooding* (ICMP *flooding*). Dengan adanya tindakan kejahatan tersebut administrator yang tidak mengerti tentang keamanan jaringan komputer atau tidak waspada dapat mencelakai dirinya. Pada sistem keaman FTP terdapat suatu kelemahan yaitu pada data username dan password yang tidak di enkripsi pada saat melakukan proses login. Dengan keadaan

tersebut membuat FTP menjadi rentan terhadap serangan oleh hacker [2]. Dari serangan seperti *brute force* FTP, *port scanning*, dan ICMP *flooding* memiliki efek yang cukup besar. Salah satu contohnya ICMP *flooding* merupakan serangan bentuk Distribute Denial-Of-Service (DDoS) yang mengancam keamanan dalam bentuk penyimpanan pada *client-server*, bentuk dari proses komunikasi *client-server* sendiri disebut *files transfer*. Aktifitas *files transfer* biasa dilakukan oleh *protocol* FTP dengan melakukan pertukaran data. FTP juga melakukan suatu layanan antar komputer dalam sebuah jaringan. Karena FTP bekerja dengan berlandaskan koneksi TCP, *protocol* FTP juga menggunakan *Open System Interconnection* (OSI) sebagai *standart files* transfer. Secara aturan, port 21 dan 20 pada FTP memakai port *Transmission Control Protocol* (TCP) untuk menjadi penghubung antara *server* dan *client* atau sebaliknya [3]

Maka dari permasalahan diatas dibutuhkan sebuah sistem keamanan jaringan yang dapat melindungi FTP serta untuk menangkal dan mencegah dari potensi serangan – serangan yang dilakukan hacker atau cracker. Keamanan Jaringan menjadi suatu komponen yang sangat penting dalam menjaga keabsahan dan kelengkapan suatu informasi data beserta penggunanya [4]. Keamanan jaringan juga berjalan untuk mengurangi dampak ancaman dari serangan baik itu langsung atau tidak langsung. Dengan begitu seorang admin memerlukan sebuah sistem yang bisa mendukung admin untuk mengantisipasi dan mengawasi jaringan dari serangan hacker atau cracker. Untuk itu diperlukan sebuah sistem yang cocok untuk mencegah dan mengidentifikasi serangan, maka digunakanlah metode *Intrusion Prevention System* (IPS) [5].

IPS mempunyai fungsi untuk mengamati *traffic* data yang berjalan secara real-time pada jaringan serta mengidentifikasi semua tindakan yang mencurigakan [6]. Metode IPS juga merupakan upgrade dari metode *Intrusion Detection System* (IDS) karena bisa melakukan monitoring dan pencegahan serangan dengan memblokir semua ancaman [7]. Dengan demikian metode IPS berperan selayaknya *firewall* yang dapat menerima atau mencegah semua paket yang mencoba masuk lalu digabungkan dengan monitoring jika terdapat data yang mencurigakan karena

konsep dari *firewall* yaitu jika ada traffic data yang masuk menuju ke jaringan *firewall* akan melakukan tindakan pemeriksaan dan pengawasan pada *traffic* tersebut [8]. Jika terjadi tindakan yang mencurigakan maka akan di indentifikasi sebagai serangan maka IPS akan melakukan tindakan pencegahan dengan memblokir serangan dengan cara block dan drop *IP Address*. Hasil dari serangan dapat ditampilkan pada log sistem MikroTik dan dapat dikirim dengan Gmail untuk sebagai monitoring alert peringatan dini untuk administrator ketika terjadi serangan pada FTP [9]. Dari latar belakang tersebut penulis mengadakan penelitian dengan judul **"ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN FILE TRANSFER PROTOCOL (FTP) MENGGUNAKAN INTRUSION PREVENTION SYSTEM (IPS) PADA MIKROTIK"**

1.2 Rumusan Masalah

Dari latar belakang masalah yang telah diuraikan diatas, maka dapat disusun rumusan masalah pada penelitian ini adalah sebagai berikut :

1. Apakah dengan mengimplementasikan *Intrusion Prevention System* (IPS) pada *firewall* MikroTik dapat mengamankan service FTP yang berada pada router MikroTik dari serangan *Brute force* FTP, ICMP *flooding*, dan *Port scanning*?
2. Berapakah waktu yang dibutuhkan *Intrusion Prevention System* (IPS) pada *firewall* router MikroTik untuk mencegah dan mengirim pesan alert serangan pada gmail?

1.3 Batasan Masalah

Pada penelitian ini penulis memberikan beberapa batasan masalah penelitian dengan tujuan pokok permasalahan yang dibahas lebih terarah dan tidak keluar dari pokok permasalahan yakni sebagai berikut:

1. Penulis mengimplementasikan metode *Intrusion Prevention System* (IPS) pada *firewall* router MikroTik.
2. Penetration testing serangan menggunakan *brute force* FTP, ICMP *flooding*, dan *Port scanning* pada kali linux.
3. Service FTP yang diamankan berada pada router MikroTik.

4. Perangkat yang dipakai untuk mengimplementasikan IPS yaitu router mikrotik RB951Ui-2HND.
5. Hasil dari percobaan serangan akan diintergrasikan dari log mikrotik ke gmail sebagai alert monitoring administrator.
6. Pengujian serangan dilakukan pada jaringan Lokal.
7. Tools yang digunakan yaitu Znmap pada windows dan VM kali linux yaitu Ncrack, xHydra dan Hping3.

1.4 Tujuan Penelitian

Tujuan dari penelitian yang ingin dicapai pada laporan ini yaitu :

1. Mengetahui dengan megimplementasikan *Intrusion Prevention System* (IPS) pada *firewall* di router MikroTik dapat mengamankan service FTP yang berada di router MikroTik dari serangan *Brute force* FTP, ICMP *flooding*, dan *Port scanning*.
2. Mengetahui dengan menggunakan *Intrusion Prevention System* (IPS) pada *firewall* MikroTik, proses *prevention* dan monitoring serangan dapat diketahui secara *real-time* dengan alert monitoring gmail.

1.5 Manfaat Penelitian

Manfaat dari penelitian diatas yaitu:

1. Untuk peneliti manfaatnya yaitu peneliti berhasil mengamankan service FTP yang berada di router MikroTik dari serangan *brute force* FTP, ICMP *flooding*, dan *Port scanning* lalu hasil serangan bisa dimonitoring memggunakan email secara *real-time*.
2. Untuk pengguna dapat merasakan manfaat dari penelitian ini yaitu pengguna bisa memakai service FTP pada router MikroTik sebagai tempat penyimpanan data dengan mengadopsi sistem keamanan yang sama seperti peneliti.

1.6 Sistematika Penulisan

Dalam melakukan penulisan penulis memakai sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisi pendahuluan yang menjabarkan latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi tinjauan pustaka dan dasar-dasar teori yang digunakan dalam pembuatan skripsi sebagai penguat.

BAB III METODE PENELITIAN

Pada bab ini didalamnya terdapat tinjauan tentang objek penelitian, analisis masalah, solusi yang ditawarkan, rancangan sistem keamanan, alur penulisan skripsi dan alur kerja sistem serangan dan pencegahan.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini merupakan tahapan yang penulis melakukan implementasi dari sistem kemananan, membuat alur dari serangan, melakukan pengujian serangan dan hasil pengujian serangan.

BAB V PENUTUP

Pada bab ini nantinya berisi kesimpulan dan saran yang didapat dari penelitian.

LAMPIRAN

Pada lampiran akan ditampilkan detail dari konfigurasi IPS dan monitoring