BAB I
PENDAHULUAN

1.1 Latar Belakang

Jumlah ancaman dan serangan keamanan siber selalu meningkat setiap saat dan seringkali standar keamanan seperti IDS *(Intrusion Detection Systems)*, *access control system* dan *firewall* tidak cukup untuk mengamankan server dari penyerang[1]. Salah satu perangkat yang paling penting pada suatu jaringan dengan cakupan yang luas adalah router. Pesatnya kemajuan teknologi router membuktikan bahwa router adalah perangkat yang paling dibutuhkan khususnya pada penyedia jasa internet dalam membangun sebuah jaringan maupun keamanannya khususnya perangkat router Miktorik. Target utama *attacker* sebelum masuk pada sistem utama atau pusat data adalah dengan mematikan kinerja router[2]. Ancaman serangan siber seperti serangan *Brute Force* dan DDoS dapat dengan mudah menyerang server maupun router. DDoS merupakan serangan yang bertujuan untuk mematikan target dengan cara memadati jalur data dengan paket yang illegal, secara serempak[3].*Brute force* merupakan ancaman dari penyerang yang mencoba untuk login dengan menggunakan protocol SSH dan telnet untuk mengungkap *password* login[4]. Penyelesaian dalam menebak *password* menggunakan algoritma *Brute Force* dapat dengan mudah mencari *password* dengan mengkombinasikan karakter dan panjang *password*[3].

UDP (*User Datagram Protocol*)- *Flooding* adalah jenis serangan yang memanfaatkan protokol UDP dengan mengurangi sambungan (*connectionless*) untuk menyerang target. UDP adalah jenis serangan yang cukup mudah dilakukan dibandingkan dengan jenis serangan lain[5].

Fitur *Firewall Rules* yang terdapat pada Mikrotik dapat diterapkan pada sistem keamanan jaringan komputer. *Firewall Rules* merupakan sekelompok sistem yang menetapkan kebijakan kendali akses antara dua jaringan, dengan prinsip sepasang mekanisme memblok lalu lintas, dan mengizinkan lalu lintas jaringan. Dengan menggunakan *firewall*, pengelola jaringan dapat membatasi hak akses terhadap IP *Address* yang dianggap kurang baik bagi pengguna jaringan.

Oleh karena itu, penulis berinisiatif untuk menganalisa jaringan wifi dari

serangan *brute force* dan udp dns *flood* menggunakan router mikrotik. Penulis akan mencegah serangan *brute force* dan udp dns *flood* dengan cara melacak ip *address* penyerang dan memblokir ip *address* tersebut sesuai dengan waktu yang ditentukan (contohnya 1 hari). Berdasarkan latar belakang yang telah diuraikan, penulis mengangkat judul "ANALISIS KINERJA JARINGAN (WIFI) DARI SERANGAN *BRUTE FORCE* DAN UDP DNS *FLOOD* DENGAN *FILTER FIREWALL* PADA ROUTER MIKROTIK".

1.2 Rumusan Masalah

Dari uraian latar belakang diatas dan untuk mendapatkan hasil yang sesuai harapan, maka dibuat rumusan masalah sebagai berikut :

1. Bagaimana proses mengamankan Jaringan Wifi dari serangan *Brute Force* dan UDP DNS *Flood* dengan *filter firewall* ?
2. Bagaimana hasil analisis pengujian kinerja dari masing masing metode yang dilakukan pada serangan *brute force* dan udp dns *flood* pada router mikrotik dengan *filter firewall* ?

1.3 Batasan Masalah

Agar penelitian ini lebih focus, maka dibuat batasan masalah sebagai berikut:

1. Pengujian yang dilakukan menggunakan laptop G40-80 Intel(R) Core(TM) i3-5005U CPU @ 2.00GHz
2. Pengujian dan Analisis ini menggunakan Mikrotik RB2011UiAS-2HnD-IN
3. Pengujian ini dilakukan pada jaringan lokal rumah.
4. Aplikasi UDP *Unicorn* digunakan untuk melakukan serangan UDP DNS *Flood*.
5. Aplikasi *PuTTY* digunakan untuk melakukan serangan *Brute force*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang diuraikan diatas, maka tujuan penelitian ini adalah sebagai berikut :

1. Untuk mengetahui dan memastikan adanya celah keamanan suatu jaringan wifi pada router Mikrotik
2. Untuk mengamankan router mikrotik dari serangan *Bruteforce* dan UDP DNS *Flood*.
3. Untuk mempermudah administrator atau pemilik jaringan dalam melakukan pencegahan secara dini sebelum adanya serangan pada perangkat router Mikrotik yang dapat menimbulkan kerusakan maupun kerugian pada pengguna.

1.5 Manfaat Penelitian

Penelitian ini untuk memperoleh manfaat dalam pengetahuan bagi pihak-pihak sebagai berikut:

a. Bagi penulis
   1. Mengerti dan memahami cara mengkonfigurasi Mikrotik RouterOS.
   2. Dapat menjadi sarana untuk melatih kemampuan yang dimiliki penulis tentang penerapan manajemen jaringan dengan menggunakan Mikrotik sehingga dapat menambah wawasan bagi penulis.
   3. Mengerti dan memahami konsep keamanan jaringan Mikrotik dan dapat diimplementasikan.
   4. Untuk memenuhi salah satu syarat kelulusan strata satu (S1) Program studi Informatika Fakultas Ilmu Komputer.
   5. Sebagai *port*ofolio untuk penulis yang berguna untuk masa yang akan datang.
   6. Sebagai tolak ukur terhadap apa yang sudah didapat oleh penulis semasa kuliah.

b. Bagi Universitas

1. Memberikan gambaran seberapa jauh mahasiswa dapat menerapkan ilmunya.
2. Dapat dijadikan referensi bagi penelitian berikutnya,khususnya dalam penanganan manajemen jaringan.

c. Bagi pembaca

1. Dapat memahami pentingnya keamanan jaringan wifi.
2. Dapat dijadikan referensi bagi penelitian berikutnya dalam melakukan pencegahan secara dini sebelum adanya serangan pada perangkat router Mikrotik yang dapat menimbulkan kerusakan maupun kerugian pada pengguna.

1.6 Metode Penelitian

Peneliti menggunakan metode penelitian dalam memperoleh data-data adalah sebagai berikut :

1.6.1 Metode Pengumpulan Data

Pengumpulan data yang dilakukan untuk kegiatan penelitian dalam Menyusun laporan ini yaitu :

1. Studi Pustaka

Pengambilan data menggunakan metode studi pustaka yaitu dengan cara mempelajari dan meneliti literatur-literatur dari sumber buku-buku, jurnal ilmiahmaupun dari internet yang berkaitan dengan topik penelitian.

1.6.2 Analysis

Tahap ini merupakan tahap awal dengan melakukan Analisa kebutuhan seperti software dan hardware. Serta menganalisa permasalahan yang muncul dalam membuat topologi jaringan *firewall* untuk diterapkan metode dalam jaringan *firewall*.

1.6.3 Design

pada tahap design ini akan membuat topologi jaringan dengan mengambil dari data-data analisis yang sudah didapatkan ditahap sebelumnya. Tahap ini meliputi penggambaran design topologi jaringan *firewall* dan jalur perkabelan dibuat lebih jelas.

1.6.4 Implementation

Pada tahap ini akan dilakukan implementasi keamanan pada jaringan secara lan berbasis vlan menggunakan semua data-data dari hasil tahap sebelumnya.

1.6.5 Monitoring

Tahap monitoring merupakan salah satu tahap penting dalam penelitian karena merupakan tahap melakukan pengamatan langsung terhadap performa kinerja dari masing-masing metode yang diterapkan dengan cara melihat hasil yang didapatkan dari tiap-tiap metode berupa keamanan dari serangan *Brute force* dan udp dns *flood*.

1.7 Sistematika Penelitian

Dalam penulisan skripsi ini dibagi menjadi lima bab dengan beberapa sub pokok bahasan, Adapun sistematika penulisan dari skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Menjelaskan tugas akhir ini secara umum, yang terdiri dari latar belakang masalah, rumusan masalah, batasan masalah,tujuan, manfaat dan sistematika penulisan.

BAB II LANDASAN TEORI

Berisi tentang teori-teori yang digunakan dalam penelitian, perancangan dan pembuatan sistem.

BAB III METODE PENELITIAN

Memaparkan secara rinci mengenai metode yang digunakan dalam pengumpulan data maupun metode pengembangan sistem yang dilakukan pada penelitian ini.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Memaparkan dari hasil-hasil tahapan penelitian, mulai dari analisis, desain,

hasil testing dan implementasinya.

BAB V PENUTUP

Menguraikan kesimpulan dari penelitian dan saran-saran sebagai bahan pertimbangan untuk penelitian selanjutnya.