BAB 1
PENDAHULUAN

1.1. Latar Belakang Masalah

Pesatnya perkembangan teknologi internet pada saat ini yang semakin terus meningkat tidak dapat dipungkiri akan berdampak pada meningkatnya *cyber crime*, seiring dengan demikian yang harus diperhatikan oleh *administrator* jaringan adalah terhadap berbagai macam serangan yang bisa dilakukan di internet oleh pihak yang tidak bertanggung jawab (Amarudin and Ulum 2018). Salah satu jenis serangan yang sering terjadi pada keamanan jaringan komputer adalah *Brute force attacks. Brute force* adalah Salah satu teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin untuk memecahkan *password*, kunci, kode atau kombinasi (Gunawan 2016). Seringkali *attacker scanning port* di server jaringan terlebih dahulu dan kemudian *attacker* melakukan *brute force* untuk mengetahui *username* dan *password admin*, *attacker* memasuki ke sebuah sistem jaringan melalui port yang terbuka seringkali memanfaatkan kelemahan dari *firewall* server jaringan.

Pada salah satu perguruan tinggi yang ada di Sumatera selatan pada Tahun 2017 pernah mendapatkan sebuah serangan yaitu pada situs *web* sehingga mengakibatkan terjadinya perubahan tampilan (*deface*). Berdasarkan data yang didapat bahwa sistem pada *server* terdapat *port* yang cukup banyak terbuka seperti pada *port* 80 *hypertext transfer protocol (http*), *port* 22 *secure shell* (*SSH*) dan *port* 21 *ftp server*. Berkaca dari kasus tersebut *administrator* harus lebih waspada lagi dalam mengamankan jaringan serta mengawasi *port-port* yang terbuka. Salah satu metode yang dapat digunakan administrator adalah *port knocking. Port knocking* sendiri merupakan konsep penting untuk mengamankan layanan yang disediakan *server*. Kegunaan untuk membuka akses ke *port* tertentu yang telah ditutup *firewall*, dengan cara mengirimkan paket atau koneksi tertentu yang bisa berupa protokol TCP, UDP maupun ICMP. koneksi yang dikirim oleh *host* sudah sesuai dengan rule *knocking* yang diterapkan, maka secara otomatis *firewall* akan memberikan akses *port* yang sudah diblok (Ernawati et al. 2022). Sehingga mempermudah *administrator* dalam mengamankan jaringan serta mengurangi kerentanan pada jaringan yang ada terutama serangan *bruteforce dan port scanning*.

Keamanan jaringan adalah proses dimana untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari pengguna yang di sebut “penyusup” yang tujuanya untuk masuk

ke dalam *server* jaringan dan mengakses setiap bagian dari sistem jaringan komputer (Devie Ryana Suchendra, Alfian Fitra Rahman 2017) Salah satu perangkat jaringan yang dapat digunakan dalam mengamankan suatu jaringan komputer adalah *routerboard mikrotik* mengingat kehandalan yang ditawarkan dan harganya sangat terjangkau. *Routerboard mikrotik* adalah perangkat jaringan komputer yang berupa *hardware software* yang dapat difungsikan sebagai *router*, sebagai alat *filtering*, *switching* dan juga untuk mengamankan jaringan komputer (Amarudin and Ulum 2018)

Berdasarkan permasalahan tersebut penelitian ini menerapkan sistem keamanan jaringan menggunakan *router mikrotik*. Sistem dikembangkan dengan memanfaatkan metode *port knocking* yang dapat menjaga keamanan *port* dan mencegah serangan sehingga server jaringan komputer keamanannya semakin bertambah dengan lapisan *port knocking* yang telah dikopnfigurasi pada bagian *firewall mikrotik*. Selain menggunakan metode *port knocking* penulis menambahkan fitur *port scan detection* yang berguna untuk memperkuat dan dapat mendeteksi terhadap serangan *port scanning* dan juga fitur pengiriman pesan *telegram* via *bot telegram* yang berguna untuk mengirimkan pesan kepada pihak administrasi apabila terdapat indikasi serangan sehingga mempermudah *administrator* jaringan dalam memantau server jaringan dan mengamankannya juga.

1.2. Rumusan Masalah

Dari latar belakang diatas, masalah dapat dirumuskan adalah :

a) Bagaimana menerapkan keamanan jaringan dengan menggunakan metode *port knocking*?
b) Apakah metode *port knocking* yang diterapkan berpengaruh terhadap serangan keamanan jaringan komputer (*Bruteforce attack* dan *Port Scanning*) ?
c) Bagaimana pengaruh fitur *port scan detection* dan notifikasi *bot telegram* terhadap proses serangan keamanan jaringan computer ?

1.3. Batasan Masalah

Agar pembahasan penelitian lebih terarah, maka masalah yang dibahas dibatasi pada beberapa hal sebagai berikut :

a) Penelitian menggunakan perangkat *routerboard mikrotik RB941-2nD Hap lite* .
b) Pengujian hanya menggunakan dua metode penyerangan yaitu *Brute force attack (Dictionary Attack)* dan *Port scanning*.

c) Pengujian serangan *Brute force attack* menggunakan *tools PuttY*.

d) Pengujian *Port scanning* menggunakan *tools Zenmap*.

1.4. Tujuan Penelitian

Penelitian ini memiliki beberapa tujuan, yaitu:

a) Penerapan metode *port knocking* untuk menjaga keamanan *port* dan mencegah serangan pada *server* jaringan komputer.

b) Memperkuat keamanan jaringan terhadap serangan *port scanning* dengan metode *port knocking*.

c) Menjaga penggunaan *remote access* dari *client* jaringan luar mauapun dalam yang tidak mempunyai hak *access* dan *router* dapat melakukan pengiriman notifikasi *bot telegram* yang terkirim langsung ke pihak *administrator* ketika terdeteksi adanya serangan.

1.5. Manfaat Penelitian

Adapun manfaat penelitian yang dapat diperoleh dari penelitian ini nantinya adalah :

a) Bagi penulis penelitian ini digunakan sebagai salah satu refrensi penambahan wawasan ataupun ide pengembangan sistem untuk para administrator dalam mengamankan jaringan.

b) Bagi peneliti selanjutnya, penelitian ini dapat digunakan sebagai salah satu refrensi dalam melakukan pengembangan terkait keamanan jaringan terutama dalam bagian pengamanan port.