BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Jaringan komputer saat ini berkembang sangat pesat. Berbagai informasi dapat kita dapatkan dengan mudah, cepat, dan akurat. Dilihat dari cepatnya perkembangan teknologi jaringan kompter saat ini yang harus diperhatikan oleh pengelolah jaringan adalah keamanan dari jaringan itu sendiri. Jaringan komputer digunakan hampir semua orang tanpa terkecuali para *cracker*. Adanya maksud dan tujuan tertentu para *cracker* melakukan penyusupan melalui *port-port* yang terdapat pada jaringan sehingga dapat merugikan para pemilik server dan jaringan komputer. Banyak organisasi yang menggunakan jaringan komputer untuk saling bertukar informasi data dan file. Sehingga menjadi kebutuhan yang sangat penting dalam mendukung kegiatan sebuah organisasi, baik yang berupah organisasi komersial (perusahaan), pergururan tinggi, lembaga pemerintahan, maupun individu (pribadi). Dengan demikian yang harus diperhatikan oleh para pengelolah jaringan ialah meningkatkan keamanan pada jaringan supaya celah-celah yang terdapat pada jaringan tidak dapat dilihat oleh orang yang tidak bertanggung jawab seperti *crecker*.

Sistem keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi pengguna yang tidak sah (penyusup) dari jaringan komputer. Tujuannya adalah untuk mengantisipasi resiko jaringan komputer yang dapat berupa ancaman fisik maupun logik. Yang dimaksud ancaman fisik itu adalah yang merusak bagian fisik komputer atau *hardware* komputer sedangkan ancaman logik yaitu berupa pencurian data atau penyusup yang membobol akun seseorang [1].

Sebagian besar para *cracker* melakukan serangan dengan mengeksploitasi port-port yang terbuka pada komputer target. Contoh serangan *DOS/DdoS (Distributed Denial of Service),* serangan ini dilakukan dengan membanjiri *host* pada komputer target dengan paket dalam jumlah besar yang berasal dari *host- host* berbeda. Tahapan yang dilakukan penyerang dalam penyerangan ialah

melakukan identifikasi komputer target. Tahap port *scanning* dimana penyerang dapat mengambil informasi port-port yang terbuka pada mesin target. Lalu tahap *OS Finger Printing* dalam tahan ini penyerang dapat mengetahui operasi sistem apa yang digunaka target dengan memahami kelakuan port yang terbuka saat membalas paket yang dikirimkan ke port tersebut. Dengan demikian yang harus diperhatikan oleh para pengelolah jaringan ialah meningkatkan keamanan pada jaringan supaya celah-celah yang terdapat pada jaringan tidak dapat dilihat oleh orang yang tidak bertanggung jawab seperti *crecker*.

Peningkatan keamanan jaringan menggunakan simple port knocking disarankan sebagai solusi mengamankan router mikrotik serta memonitoring jaringan melalui pembatasan akses blocking pada port yang terdapat pada jaringan tersebut. Simple port knocking diterapkan agar sistem yang dibangun mampu mendeteksi dan menghindari serangan yang berbahaya terhadap jaringan dan langsung memberikan peringatan kepada pengelola jaringan (administrator) tentang kondisi jaringan yang sedang berjalan pada saat kejadian berlangsung, Penerapan *simple port knocking* menggunakan media *router mikrotik* yang berfungsi untuk merubah konfigurasi setting dan proteksi *router* sehingga tatap aman dari serangan *cracker* [2].

Port knocking merupakan suatu sistem keamanan yang bertujuan untuk membuka atau menutup akses *block* ke *port* tertentu dengan menggunakan *firewall* pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi berupa protokol TCP, UDP, maupun ICMP. Sehingga untuk masuk dan menggunakan akses ke port tertentu yang telah dibatasi, maka *user* harus mengetuk terlebih dahulu dengan memasukan *rule* yang harus dilakukan terlebih dahulu. *Rule* yang mana hanya diketahui oleh pihak penyedia jaringan (administrator jaringan). Sebuah sistem harus memiliki keseimbangan antara keamanan dan fleksibelitas. Satu cara untuk mencapai sistem seperti demikian yaitu dengan menggunakan akses *firewall*. Dengan menggunakan *firewall* maka secara tidak langsung kita dapat mendefiniskan *user* yang dapat dipercaya dan yang tidak dapat dipercaya dengan menggunkan alaat IP sebagai kriteria filter [3].

Kelemahan dari *firewall* adalah tidak dapat membedakan *user* yang dapat dipercaya. Karena *firewall* hanya dapat membedakan alamat IP yang diasumsikan digunakan oleh orang yang tidak dapat dipercaya. agar dapat meningkatkan keamanan yang dibutuhkan dan mampu untuk mengizinkan *user* yang dapat dipercaya untuk mengakses sebuah *server* atau jaringan maka diperlukan suatu metode yang dapat memenuhi syarat kebutuhan tersebut. Salah satu metode yang dapat diterapkan untuk memenuhi kebutuhan tersebut adalah dengan menggunakan metode *simple port knocking.*

Konfigurasi *routing* pada router dapat menggunakan *static routing* atau *dynamic routing*. Untuk jaringan komputer yang tidak terlalu besar, penggunaan *static routing* bisa dilakukan karena konfigurasinya tidak terlalu sulit dan tidak memakan banyak sumber daya. Namun jika digunakan pada jaringan komputer berukuran besar *static routing* akan menyulitkan *administrator* yang bertugas untuk mengatur dan menjaga konfigurasi *table routing* agar komunikasi dalam jaringan tersebut tetap dapat dilakukan. untuk itu, digunakanlah *dynamic routing* untuk melengkapi proses *routing* pada jaringan secara otomatis, mempermudah konfigurasi koneksi antar jaringan, dan membantu pekerjaan dari *administrator* jaringan [4]

Dynamic Routing adalah proses pengisian data *routing table* secara otomatis. Apabila jaringan memiliki lebih dari satu kemungkinan rute untuk tujuan yang sama maka perlu digunakan *dynamic routing.* Protokol *routing* mengatur router-router sehingga berkomunikasi satu dengan yang lain dan memberikan informasi *routing* yang dapat mengubah isi *forwarding table,* tergantung keadaan jaringannya. Sehingga router-router dapat mengetahui keadaan jaringan yang terakhir dan mampu meneruskan datagram ke arah yang benar [5].

Adapun dalam pembuatan laporan ini penulis mengambil beberapa penelitian terdahulu antara lain penelitan yang dilakukan oleh Iga Revva Princess Jeinever, Abdul Rasyidm, Nugroho Suharto pada tahun 2018 mengenai Penerapan **"Sistem Keamanan Jaringan Menggunakan *Random Port Knocking* Berbasis *Raspberry* Pi Yang Dikirm Melewati Telegram".** Penelitian ini membahasa tentang *Random port Knocking* merupakan cara yang tepat dan dapat dipakai

untuk meningkatkan keamanan jaringan [6]. Penelitian selanjutnya yaitu penelitian dari Devie Ryana Suchendra, alfian Fitra Rahman, Setia Juli Irzal Ismail pada tahun 2017 mengenai **"Penerapan Sistem Pengamanan *Port* Pada Layanan Jaringan Menggunakan *Port Knocking"*** membahas tentang keamanan akses dan *port*, layanan jaringan yang alan dibangun di sistem operasi Linux Ubuntu 14.04 [7]. Penelitian berikutnya yaitu penelitian oleh Nasrul Firdaus, angga fitriawan pada tahun 2018 mengenai **"Implementasi Keamanan *Mikrotik* Mengunakan *Metode Simple Port Knocking* Pada Sman 1 Ngantang"** membahas tenang keamanan *mikrotik* dengan menggunakan metode *Simple Port* Knocking dapat meningkatkan keamanan *mikrotik* dalam serangan *Brute Force* [8]. Penelitian yang terkait berikutnya yaitu penelitian oleh aprianto Puji Adi Kusuma, asmunin pada tahun 2016 mengenai **"Implementasi *Simple Port Knocking Pada Dynamic Routing (Ospf)* Menggunakan Simulasi Gns3"** yang membahas tentang implementasi menggunakan metode *simple port knocking* untuk memberikan akses filter pada *firewall*, bertujuan memberikan keamanan untuk pengguna akses komputer [9] . Penelitian yang terakhir selanjutnya yaiti penelitian oleh Amarudin tahun 2018 mengenai **"Analisis Dan Implementasi Keamanan Jaringan Pada *Mikrotik* Router Os Menggunakan Metode *Port Knocking*"** Membahas tentang sebuah protocol pada *firewall* yang disebut dengan *Port Knocking*. Dimana fungsi *Port Knocking* ini adalah untuk menjaga hak akses perangkat Router dari pengguna yang tidak berwenang untuk mengaksesnya

Berdasarkan latar belakang tersebut, maka peneliti tertarik mengangkat permasalahan ini kedalam penelitian yang berjudul **"IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN METODE *PORT KNOCKING* PADA ROUTER MIKROTIK DI PAPINKA VALLEY PANGKALPINANG"**

1.2. Perumusan Masalah

Berdasarkan dari latar belakang diatas, maka rumusan masalahnya sebagai berikut :

1. Bagaimana meningkatkan keamanan jaringan komputer menggunakan metode *simple port knocking* ?
2. Bagaimana melakukan *port knocking* pada RouterBoard Mikrotik.
3. Bagaimana seorang administrator jaringan dapat memonitor jaringan?

1.3. Batasan Masalah

Agar pembahasan lebih terarah dan tidak menyimpang dari yang direncanakan sebelumnya, maka peneliti hanya membahas bagaimana penerapan metode *simple port knocking* pada *dynamic routing* menggunakan *Router Mikrotik.*

1. Penulis hanya mengimplementasikan *Port Knocking* pada *RouterBoard Mikrotik.*
2. Penulis menggunakan 1 laptop untuk mengimplementasikan.
3. Dalam pengujian pengetukan *port* penulis menggunakan aplikasi PuTTY.

1.4. Tujuan dan Manfaat Penelitian

1.4.1. Tujuan Penelitian

Tujuan dari penelitian ini yaitu :

1. Untuk meningkatkan keamanan jaringan komputer.
2. Untuk mengurangi terjadinya serangan pada komputer.
3. Untuk mencegah dan mengindentifikasi penggunaan yang tidak sah dari jaringan komputer.

1.4.2. Manfaat Penelitian

Adapun manfaat penelitian ini sebagai berikut :

1. Untuk membantu mengamankan jaringan komputer.

2. Untuk mempermudah banyak organisasi saling bertukar informasi tanpa perlu khawatir adanya gangguan serangan *cracker*.
3. Sebagai solusi mengamankan *Router OS Mikrotik* serta memonitoring jaringan computer.

1.5. Sistematika Penulisan

Sistematika penulisan skripsi ini dibuat agar dapat menjadi pedoman atau garis besar penulisan laporan penulisan ini dan dapat menggambarkan secara jelas isi dari laporan penelitian sehingga terlihat hubungan antara bab awal hingga bab terakhir. Sistem penulisan laporan penelitian ini terdiri dari :

BAB I PENDAHULUAN

Pada bab ini penulis memberikan gambaran secara jelas mengenai latar belakang permasalahan, rumusan masalah, tujuan, manfaat, pembatasan masalah, metode penelitian dan sistematikan penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisikan teori – teori dan referensi tentang Jaringan Komputer, Keamanan Jaringan, *Port Knocking, Firewall, Router, Mikrotik, OSI (Open System Interconnetion), NAT (Network Address Translation), Dynamic Routing, TCP/IP* dan landasan teori yang menjadikan dasar yang digunakan untuk penelitian ini. Pada bab ini akan diterapkan secara detail mengenai informasi studi pustaka yang diperoleh oleh peneliti yang berkaitan dengan meningkatkan keamanan jaringan dengan *simple port knocking* pada *dynamic routing.*

BAB III ANALISIS DAN PERANCANGAN

Pada bab ini membahas tentang analisis keamanan jaringan komputer dengan *Simple Port Knocking* dan perancangan untuk melakukan penelitian meningkatkan keamanan jaringan dengan *simple port knocking* serta topologi jaringan yang digunakan.

BAB IV HASIL DAN EVALUASI

Pada bab ini berisikan hasil dari penerapan jaringan *simple port knocking* dan evaluasi dari kinerja jaringan yang telah diterapkan.

BAB V KESIMPULAN

Pada bab ini berisi kesimpulan–kesimpulan yang didapat dari hasil penelitian dan saran-saran untuk perbaikan/mengevaluasi terhadap apa yang telah dijelaskan sebelumnya.