BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer saat ini berkembang sangat pesat. Berbagai informasi dapat kita dapatkan dengan muda, 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 *crecker* 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.(Abrianingsih & Aksara, 2017)

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.*

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.

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. (Wijaya, 2011)

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 (Ahmad, 2015)

Berdasarkan latar belakang tersebut, maka peneliti tertarik mengangkat permasalahan ini kedalam penelitian yang berjudul **“ MENINGKATKAN KEAMANAN JARINGAN DENGAN *SIMPLE PORT KNOCKING* PADA *DYNAMIC ROUTING*”**

1.2 Perumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalahnya sebagai berikut :

1. Bagaimana meningkatkan keamanan jaringan komputer menggunakan metode *simple port knocking.*
2. Bagaimana melakukan *remote* jaringan dengan menggunakan metode *simple port knocking*.
3. Bagaimana perbandingan *Mikrotik* yang menggunakan metode *simple port knocking* dangan yang tidak menggunakan *simple port knocking*.

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.*

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Tujuan dari penelitian ini yaitu Meningkatkan keamanan jaringan komputer dengan menerapkan metode *simple port knocking* supaya sistem dapat mendeteksi dan menghindari serangan berbahaya dari *cracker.*

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 komputer.

1.5 Waktu dan Tempat

1.5.1 Waktu Penelitian

Penelitian ini akan dilakukan pada jam semester genap Tahun Akademik 2018-2019, yaitu bukan April 2019 sampai bulan Agustus 2019. Peneltian dilakukan pada jam 09.00-16.00.

1.5.2 Tempat Penelitian

Penelitian akan dilakukan di Laboratorium Cisco Kampus C Universitas Bina Darma Palembang.

1.6 Metodologi Penelitian

Metode yang digunakan pada penelitian ini yaitu metode PPDIOO yang dikembangkan oleh CISCO dalam desain sistem jaringan, karena dalam penelitian ini dilakukan peningkatan keamanan jaringan *simple port knocking* pada *dynamic routing.*

Menurut (Bruno, jordan, 2011: 11), cisco telah menghasilkan sebuah formula siklus hidup perencanaan jaringan, menjadi enak fase: prepare(persiapan), Plan (perencanaan), Design (Desain), Implement (Implementasi), Operate (Operasi) dan Optimize (Optimasi). Fase-fase ini dikenal dengan istilah PPDIOO.

1. *Prepare* (Persiapan)

   Pada tahap persiapan ini peneliti akan menyiapkan beberapa alat-alat yang dibutuhkan dalam penerapan sistem keamanan pada jaringan dengan metode *Simple Port Knocking,* yang akan dijelaskan pada bab III.

2. *Plan* (Perencanaan)

   Pada tahap perencanaan ini peneliti melakukan rancangan jaringan yang digunakan dalam penerapan sistem peningkatan keamanan jaringan dengan metode *Simple Port Knocking.* dimana pada tahap ini peneliti akan merencanakan IP dan Routing yang akan digunakan dalam sistem yang dirancang.

3. *Design* (Desain)

   Pada tahap ini dimana peneliti akan mendesain topologi alur kerja dari sistem keamanan jaringan *Simple Port Knocking* yang akan di terapkan.

4. *Implement* (Implementasi)

   Pada tahap ini peneliti akan menerapkan sistem yang akan direncanakan pada tahap-tahapan sebelumnya dengan melakukan simulasi pada *Sofware* GNS3 guna tercapainya hasil yang maksimal ketika diterapkan langsung menggunakan alat-alat yang asli.

5. *Operate* (Operasi)

   Pada tahap ini peneliti akan melakukan operasi pada sistem yang telah dirancang pada tahap *Implement* (Menerapkan) dimana pada tahap ini peneliti akan memantau jaringan yang telah diterapkan mulai dari kinerja jaringan, konfigurasi dan stabilitas jaringan.

6. *Optimize* (Optimasi)

   Pada tahap ini dimana peneliti akan melakukan analisa dari hasil perolehan data dan melakukan identifikasi terhadap sistem yang sudah diterapkan apakah sistem sudah berjalan sesuai dengan apa yang di

inginkan atau masih perlu perbaikan lagi untuk lebih meningkatakan keamanan jaringan yang diterapkan.

1.7 Metodologi Pengumpulan Data

Metode pengumpulan data yang dilakukan pada penelitian ini adalah sebagai berikut :

1. Pengamatan (*Observasi*)

   Penulis mengumpulkan data-data dan informasi dengan langsung melakukan pengamatan atau eksperimen pada objek yang ditinjau agar data tersebut bukan data manipulasi sehingga penelitian ini benar-benar mendapatkan data yang sesungguhnya.

2. Pengujian (*Testing*)

   Penulis melakukan pengujian langsung pada objek dimulai dari implementasi *simple port knocking* pada *dynamic routing*, pengujian disaat jaringan normal, pengujian jaringan putus dengan *disable port* (*bloking port*) , dan pengujian jaringan *open* akses *port* yang sebelumnya *disable port* (sesudah diberi ketukan).

3. Studi Pustaka (*Literatur*)

   Dalam metode ini penulis mendapatkan data dan informasi melalui buku, jurnal, dan internet yang berhubungan dengan objek.

1.8 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 TIJAUAN PUSTAKA

Pada bab ini berisikan teori – teori dan referensi tentang *Port Knocking*, *Firewall*, *Mikrotik*, *Port*, *OSI (Open System Interconnetion)*, *Router*, *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.