

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era globalisasi saat ini, perkembangan teknologi telah berkembang sangat pesat, hal ini dapat dilihat dari teknologi yang awalnya manual kini telah digantikan dengan alat modern seperti *smartphone*, komputer, laptop dan alat teknologi lainnya yang dapat memudahkan suatu pekerjaan. Dengan persaingan yang semakin global, suatu sistem informasi sangat dibutuhkan guna menciptakan informasi yang efektif sehingga manajemen memiliki pengetahuan untuk mendeteksi kapan perubahan kondisi membutuhkan tanggapan yang strategis. *Malware, trojan, virus*, dan pemindaian *port* adalah beberapa dari risiko keamanan yang sering ditemukan untuk menemukan *port* komputer yang terbuka [1].

Keamanan jaringan komputer sangat erat kaitannya dengan keamanan informasi, sehingga keamanan jaringan sangat penting untuk melindungi informasi dari serangan berbagai pihak yang tidak bertanggung jawab. Serangan tersebut dapat ditujukan terhadap instansi, perusahaan atau lembaga tertentu, tidak terkecuali Sekolah Menengah Atas Negeri 1 Sungailiat yang dapat mengalami hal tersebut. Mengingat perkembangan teknologi informasi yang terus berubah, membuat keamanan informasi menjadi sangat penting. *Port* terbuka sering menjadi sasaran beberapa serangan sehingga orang yang tidak memiliki izin akses atau tidak berkepentingan nantinya dapat dengan mudah mengelola port yang telah mereka akses.

Sistem keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi pengguna yang tidak sah seperti 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. Peningkatan keamanan jaringan menggunakan *Simple Port Knocking* disarankan sebagai solusi mengamankan *router mikrotik* serta memonitoring jaringan melalui

pembatasan akses 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 administrator jaringan 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].

Metode *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. Protokol untuk koneksi dapat berupa *protokol TCP, UDP* atau *ICMP*. Jadi, untuk mengakses beberapa *port* yang dibatasi dan menggunakan aksesnya, user harus terlebih dahulu mengetuk *rule* yang harus dilakukan terlebih dahulu. *Rule* yang hanya diketahui oleh administrator jaringan. Sistem harus memiliki keseimbangan antara keamanan dan fleksibilitas. Salah satu cara untuk mencapai sistem tersebut adalah dengan menggunakan *firewall*. Dengan menggunakan *firewall*, maka secara langsung kita dapat mendefinisikan *user* yang dapat dipercaya dan yang tidak dapat dipercaya dengan menggunakan alamat IP sebagai kriteria filter [3].

Firewall merupakan sebuah sistem atau perangkat yang memberi otorisasi pada lalu lintas jaringan komputer yang dianggapnya aman untuk melaluinya dan melakukan pencegahan terhadap jaringan yang dianggap tidak aman. *Firewall* berada diantara kedua jaringan seperti internet dan komputer. Didalam *router mikrotik* terdapat fitur *firewall* yang berfungsi untuk melindungi dengan cara memutus atau menerima sebuah paket yang akan masuk, melewati, atau keluar *router*. *Firewall* yang bisa diterapkan untuk melindungi serangan dari para *hacker* adalah *Port Knocking*. Kelemahan dari *firewall* adalah tidak dapat membedakan *user* mana yang dapat dipercaya. Karena *firewall* hanya mampu membedakan alamat IP yang diasumsikan digunakan oleh orang yang tidak dapat dipercaya. Mencapai tingkat keamanan yang diperlukan dan mengizinkan *user* tepercaya mengakses *server* atau jaringan memerlukan metode yang memenuhi kedua kriteria

ini. Salah satu metode baru yang dirancang untuk memenuhi kedua kriteria tersebut adalah metode *Simple Port Knocking* [3]. Kelebihan dari *Port Knocking* dengan *Firewall* adalah meskipun semua *port* yang tersedia ditutup, *user* dengan hak akses yang mengetahui *port* mana yang terbuka oleh *Knocking* tetap dapat menggunakan *port* yang telah ia buka[4].

Dari latar belakang tersebut, maka penulis berkeinginan untuk mengangkat permasalahan ini kedalam penelitian yang berjudul **“RANCANG BANGUN KEAMANAN JARINGAN KOMPUTER DENGAN MENGGUNAKAN METODE *PORT KNOCKING* DI SMAN 1 SUNGAILIAT”**.

Adapun penelitian yang menjadi acuan dalam penulisan skripsi ini antara lain, penelitian yang dilakukan oleh Abdul Jamalul'ain, Odi Nurdiawan, Martanto pada tahun 2022 mengenai “Optimasi Keamanan Jaringan Komputer Menggunakan Metode *Port Knocking* Berbasis *Mikrotik* (Studi Kasus: CV. Mitra Indexindo Pratama)”[5], Penelitian selanjutnya yaitu penelitian dari Rizka Albar, Rian Okta Putra pada tahun 2022 mengenai “Analisis Keamanan Jaringan Menggunakan Metode *Sniffing* Dan Implementasi Keamanan Jaringan Pada *Mikrotik Router OS V6.48.3* Menggunakan Metode *Port Knocking*”[6], Selanjutnya penelitian oleh Rosalia Ernawati, Ikhwan Ruslianto, Syamsul Bahri pada tahun 2022 mengenai “Implementasi Metode *Port Knocking* Pada Sistem Keamanan *Server Ubuntu Virtual* Berbasis *Web Monitoring*”[7], Penelitian selanjutnya yaitu penelitian oleh Yudi Mulyanto, M.Julkarnain, Aldela Jabi Afahar pada tahun 2021 mengenai “Implementasi *Port Knocking* Untuk Keamanan Jaringan SMKN 1 Sumbawa Besar”[8], Selanjutnya penelitian oleh M.Zhafir Rifqi, Muhammad Syahroni, Misriana pada tahun 2021 mengenai “Implementasi Sistem Keamanan Jaringan Pada *Mikrotik RB-951* Menggunakan Metode *Port Knocking*”[9].

1.2 Rumusan Masalah

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

1. Bagaimana Metode *Port Knocking* bisa mengamankan akses *port* komunikasi yang terbuka untuk dimasuki dan masih tetap dapat

diakses dari luar?

2. Bagaimana meningkatkan keamanan jaringan komputer dengan menggunakan Metode *Port Knocking*?
3. Bagaimana seorang administrator jaringan dalam mengamankan *RouterBoard Mikrotik*?

1.3 Tujuan dan Manfaat Penelitian

Dibawah ini tujuan dan manfaat penelitian adalah sebagai berikut :

1.3.1 Tujuan Penelitian

Adapun tujuan penelitian ini sebagai berikut :

1. Menggunakan Metode *Port Knocking* untuk meningkatkan keamanan *router mikrotik* di jaringan SMAN 1 Sungailiat.
2. Untuk mengurangi frekuensi serangan pada *routerboard* untuk *mikrotik*.
3. Untuk menghentikan percobaan masuk ke sistem *mikrotik* yang melanggar hukum dan untuk memperkuat keamanan.

1.3.2 Manfaat Penelitian

Adapun manfaat penelitian ini sebagai berikut :

1. Dapat mengoptimalkan keamanan jaringan komputer.
2. Sebagai solusi untuk mengamankan *router mikrotik* serta menentukan port mana yang dapat di akses dan tidaknya.
3. Dapat meningkatkan rasa aman bagi pengguna *router mikrotik*.

1.4 Batasan Masalah

Adapun batasan masalah yang dibatasi agar lebih terarah dan tidak menyimpang dari pembahasan, maka peneliti hanya membahas pada rancang bangun keamanan jaringan komputer dengan menggunakan metode *port knocking* sebagai berikut :

1. Pengujian untuk *client* yang akan memasuki *port* yang telah ditentukan sudah diberikan langkah-langkahnya.

2. Penulis hanya mengimplementasikan *Port Knocking* pada *RouterBoard Mikrotik*.
3. Dalam pengujian pengetukan *port*, penulis menggunakan *Software PuTTY* dan *Software Winbox*.
4. Penulis hanya menggunakan 1 laptop untuk mengimplentasinya.
5. Pengujian hanya menggunakan 1 *client*.

1.5 Sistematika Penulisan

Sistematika penulisan skripsi ini dibagi menjadi lima bab, adapun susunan dari uraian bab-bab tersebut adalah sebagai berikut :

BAB I : PENDAHULUAN

Bab ini berisikan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini berisikan tentang penjelasan landasan teori-teori, pendapat dan sumber-sumber lain untuk mendukung dalam pembuatan laporan serta dapat digunakan sebagai acuan dalam pembahasan masalah.

BAB III : METODOLOGI PENELITIAN

Bab ini berisikan tentang pembahasan metode penelitian yang akan digunakan serta langkah-langkah yang digunakan terkait dengan penelitian yang dilakukan.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini berisikan tentang penjelasan latar belakang organisasi, struktur organisasi, jabaran tugas dan wewenang, analisis masalah sistem yang berjalan, identifikasi sistem usulan, analisis kebutuhan sistem usulan, analisis sistem, perancangan sistem hasil dan pengujian.

BAB V : PENUTUP

Bab ini berisikan tentang kesimpulan dan saran tentang keseluruhan laporan terhadap peneliti yang diperoleh dan menarik kesimpulan dari hasil yang dikerjakan dan layak untuk di implementasikan.

