BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam hal pengelolaan *server*, biasanya *administrator* sistem tidak selalu harus berada dalam ruang *server*. Hal ini karena biasanya ruangan *server* dirancang agar memiliki suhu yang cukup dingin dan stabil, dimana hal itu tentu kurang baik untuk tubuh. Sehingga biasanya seorang *administrator* menjalankan tugasnya dari luar ruang *server* dengan melalui aplikasi *remote server.* Dengan demikian seorang *administrator* cukup melakukan proses autentikasi ke *server* tersebut dan jika berhasil maka *administrator* tersebut akan mendapatkan akses untuk mengelola *server* (Suchendra, 2017).

Berbagai metode maupun jumlah serangan pada suatu *server* semakin hari semakin meningkat. Terbukanya beberapa *port* yang *listen* secara tidak langsung akan mengundang para *attacker* maupun pihak-pihak tertentu yang tidak bertanggung jawab untuk menerobos masuk ke dalam *server* melalui *port* tersebut. Hal yang sering dilakukan oleh para *attacker* adalah mencoba untuk mengeksploitasi berbagai aplikasi yang sedang *running* melalui *port* yang terbuka pada sisi *server.* Untuk mencegah hal-hal yang tidak diinginkan, biasanya *administrator* akan memasang *firewall* dan melakukan beberapa *konfigurasi* yang pada intinya adalah untuk membatasi siapapun yang akan mengakses *server.* Terbukanya *port* pada *server,* terutama *port* untuk aplikasi *remote server,* tentu akan menjadi pusat perhatian *attacker* untuk dieskploitasi.

Port knocking hadir sebagai salah satu metode autentikasi yang dapat digunakan untuk mengatasi masalah di atas. Metode ini memiliki kemampuan untuk menentukan siapa yang memang benar-benar berhak mengakses *server* (Mahmud, 2018).

Port knocking melakukan pengetukan terhadap *port-port* komunikasi yang ada dalam sistem komunikasi data. Fungsi dan cara kerja dari sistem ini tidak jauh berbeda dengan arti harafiahnya. *Port knocking* merupakan sebuah metode untuk membangun komunikasi dari mana saja, dengan perangkat komputer yang tidak membuka *port* komunikasi apapun secara bebas. Dengan kata lain, perangkat komputer ini tidak memiliki *port* komunikasi yang terbuka bebas untuk dimasuki, tetapi perangkat ini masih tetap dapat diakses dari luar. Ini dapat terjadi jika menggunakan metode *port knocking*. Koneksi dapat terjadi dengan menggunakan metode pengetukan *port-port* komunikasi yang ada. Pengetukan port-port ini dilakukan dengan kombinasi tertentu secara berurutan dalam satu rentan waktu tertentu.

Jika dilihat sesaat, *port knocking* memang tidak terlalu banyak gunanya dan tidak terlalu istimewa. Hanya melakukan buka tutup *port* komunikasi saja tentu tidaklah terlalu banyak gunanya bagi pengguna jaringan lokal. Namun bagi para pekerja jarak jauh, para pengguna komputer yang sering bekerja di luar kantor atau para *administrator* jaringan dan *server* yang harus mengurusi *server-server* mereka 24 jam dari mana saja, *port knocking* merupakan metode yang luar biasa sebagai sebuah jalan penghubung ke perangkat-perangkat komputer mereka. *Port knocking* cocok untuk mereka yang masih ingin memperkuat sistem keamanan komputer dan perangkat jaringannya, sementara tetap pula ingin

memiliki koneksi pribadi ke dalamnya secara kontinyu dan dapat dilakukan dari mana saja (Amarudin, 2018).

Jika hanya ingin membangun koneksi secara pribadi dari mana saja, mengapa tidak menggunakan *Virtual Private Network* atau VPN saja? Mungkin ada juga pertanyaan seperti itu diajukan terhadap teknologi *port knocking*. VPN memang teknologi yang selama ini digunakan untuk membangun koneksi yang bersifat *private* dari mana saja di seluruh dunia. Melalui VPN, *admin* dapat terkoneksi dengan *server-server* di kantor pusat meskipun berada di luar kota maupun luar negeri, asalkan ada koneksi *internet*. VPN bekerja dengan membangun sebuah terowongan atau sering disebut dengan istilah *tunnel*.

Untuk membuat VPN, biasanya dibutuhkan sebuah *server* atau *hardware* spesifik yang memiliki kemampuan itu. Jika *server* yang digunakan, mungkin *server* tersebut harus dipasang dengan berbagai macam aplikasi dengan berbagai pengaturan khusus dan spesifikasi tertentu, hal itu akan memakan waktu cukup lama untuk menyiapkannya. Jika menggunakan *hardware* khusus tentu akan lebih mudah, tetapi harus mengeluarkan biaya tambahan untuk itu. Membuat sistem *port knocking* jauh lebih mudah daripada membuat VPN. Fungsi dan keunggulannya banyak memiliki persamaan, meskipun cara kerja dan metode yang digunakannya sangat jauh berbeda. Untuk menghubungkan ke jaringan, *port knocking* dapat digunakan untuk membuka *service-service* tertentu yang dapat digunakan untuk melakukan *remote login*.

Port knocking pada penelitian ini dikonfigurasi dan dibangun pada *router* yang berbasis mikrotik. Pemilihan *router* mikrotik dikarenakan *router* mikrotik sangat mudah didapatkan dengan harga yang terjangkau. Dari segi pengoperasian

atau *remote*, mikrotik tergolong *user friendly* karena bantuan aplikasi winbox yang mempunyai tampilan Graphical User Interface (GUI), daripada menggunakan router bersistem operasi freeBSD atau yang lainnya yang masih berupa Command Line Interface (CLI). Penggunaan yang mudah serta didukung fitur-fitur yang menarik membuat router mikrotik banyak digunakan untuk segmen jaringan kelas kecil dan menengah. Mikrotik juga bisa mendeteksi berbagai macam *ethernet card* dari berbagai *vendor* yang berbeda (Wilman, 2017).

Oleh karena itu berdasarkan latar belakang masalah tersebut diatas, maka perlu untuk mengangkat judul **"Implementasi Sistem Keamanan Jaringan Pada Server Dengan Metode Port Knocking Berbasis Mikrotik Router OS"**.

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang yang telah diajukan, maka permasalahan yang akan dikaji dalam penulisan ini dapat dirumuskan sebagai berikut :

1. Bagaimana merancang sistem autentikasi *remote server* dengan menggunakan metode *port knocking*?
2. Bagaimana metode yang digunakan *port knocking* untuk mengatasi bentuk serangan terhadap *server*?
3. Bagaimana perbandingan tingkat keamanan *server* yang tidak menggunakan metode *port knocking* dan yang menggunakan metode *port knocking*?

1.3 Batasan Masalah

Pembahasan mengenai sistem keamanan jaringan secara detail merupakan pembahasan yang luas dan memiliki pembagian-pembagian yang sangat kompleks. Batasan-batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Metode yang digunakan adalah *port knocking*.
2. *Router* berbasis *mikrotik* dan *server* berbasis *linux ubuntu*.
3. Port yang digunakan dalam penelitian adalah port 22, 23, dan 80.

1.4 Tujuan

Adapun tujuan penelitian ini adalah sebagai berikut :

1. Merancang autentikasi *remote server* yang lebih aman yaitu dengan menggunakan metode *port knocking*.
2. Dapat melindungi *server* dari serangan pihak yang tidak bertanggung jawab dengan penerapan metode *port knocking*.
3. Mengetahui tingkat keamanan atas implementasi sistem keamanan jaringan yang telah dibangun menggunakan metode *port knocking*.

1.5 Manfaat

Penelitian ini diharapkan dapat memberikan manfaat bagi beberapa pihak. Manfaat yang pertama bagi UPN “Veteran” Jawa Timur yaitu dihasilkan sebuah sistem keamanan jaringan dengan metode *port knocking*.

Selain itu, semoga penelitian ini dapat bermanfaat bagi penulis dalam menerapkan dan mengaplikasikan ilmu pengetahuan yang diperoleh untuk mengatasi masalah-masalah yang ada pada lingkungan kerja.

Bagi akademis, hasil penulisan ini semoga dapat dijadikan referensi bagi mahasiswa lain yang juga sedang mengadakan penelitian dengan permasalahan yang sama.