BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada masa sekarang ini keamanan jaringan menjadi hal yang sangat penting dan harus diperhatikan, karena pada dasarnya jaringan yang terhubung ke internet tidak aman dan akan selalu terancam oleh serangan hacker. Dalam proses transmisi data akan melewati beberapa terminal untuk sampai ke tujuan[1]. Dengan begitu orang yang tidak bertanggung jawab dapat melakukan penyadapan atau mengubah isi dari data yang di transmisikan tersebut. Oleh karena itu diperlukan sebuah sistem keamanan jaringan sebagai bentuk pencegahan dari serangan tersebut.

Berdasarkan sebuah jurnal, salah satu serangan dari hacker yang cukup berbahaya adalah *sniffing*. Serangan ini akan mengancam akses login, dengan menangkap semua lalu lintas masuk dan keluar, termasuk *username* dan *password* atau data sensitif lainnya[1]. Karena jika hacker sudah mendapat *username* dan *password* sudah pasti hacker tersebut akan mengubah nya kemudian pengguna akan kehilangan akses-nya. Salah satu penyebab dari terjadi nya serangan tersebut adalah *port* yang terbuka.

Keamanan akses dan *port* menjadi hal yang sangat penting dalam layanan jaringan, hal tersebut menjadi satu kesatuan didalam sebuah layanan tersebut. Permasalahan keamanan jaringan sering terjadi disebabkan adanya *port* yang terbuka atau akses yang illegal, secara autentikasi dan otoriasasi dapat mengakibatkan mudahnya user yang tidak valid dapat mengakses sistem tersebut secara illegal[2]. Dengan adanya permasalahan yang dapat mengancam akses login, karena *port* yang terbuka maka diperlukan suatu implementasi metode jaringan yang dapat memberikan keamanan pada penggunanya.

Dalam penelelitian ini akan menggunakan metode port knocking sebagai solusi untuk mengatasi permasalahan tersebut. Metode *port knocking* berfungsi untuk menutup seluruh akses pada *port* tertentu dan seorang *client* dapat mengakses pada *port* tersebut ketika telah berhasil melakukan serangkaian ketukan *port* kepada

beberapa *port* yang telah diatur sebelumnnya[3]. Tujuan utamanya adalah untuk melindungi dari serangan *port scanning*, *sniffing* dan *brute force* untuk mendapat username dan password atau akses login, sehingga hanya pengguna sebenarnya yang bisa mengakses secara penuh untuk melakukan konfigurasi dan monitoring jaringan pada perangkat router. Dengan begitu akses login dapat terlindungi dari user yang tidak bertanggung jawab untuk melakukan *login* atau dalam hal ini hacker yang mendapat akses *login* melalui cara *sniffing*.

Penelitian ini juga berguna untuk melihat seberapa tangguh kemampuan hardware maupun software dari perangkat Router Mikrotik RB941 yang menggunakan Router OS versi 6.48.6 dengan Router OS license level 4. Pemilihan router tersebut sebagai objek dalam penelitian ini adalah kerena perangkat tersebut memiliki spesifikasi hardware berupa RAM 32MB yang cukup handal untuk mencegah serangan dari bruteforce. Router OS yang digunakan tersebut merupakan versi bawaan dari pabrik yang belum di update sejak perangkat router tersebut di rilis, sehingga nantinya akan dilakukan pengujian apakah software OS tersebut masih mampu melindungi dari berbagai serangan di masa sekarang ini.

1.2 Rumusan Masalah

1. Apa dampak yang ditimbulkan dari serangan *sniffing* pada Router Mikrotik RB941?
2. Bagaimana hasil pengujian yang di dapat pada setiap *port* saat metode *port knocking* di implementasikan pada router?

1.3 Batasan Masalah

1. Penyerang harus mendapatkan akses ke wifi terlebih dahulu sebelum melakukan serangan.
2. Penelitian ini menggunakan perangkat router Mikrotik RB941 dengan Router OS versi 6.48.6 yang memiliki Router OS license level 4.

3. Penelitian ini hanya menerapkan metode port knocking sebagai perlindungan terhadap *firewall* pada router.
4. Penelitian ini hanya membatasi jenis serangan *port scanning*, *sniffing* dan *brute force*.
5. Port yang digunakan untuk pengujian adalah *Port 21* (FTP), *Port 22* (SSH) *Port 23* (telnet), *Port 80* (WebFig), *Port 8291* (Winbox).

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh penulis dalam penelitian ini adalah :

1. Membuat rule konfigurasi pada firewall untuk mencegah dampak dari serangan *sniffing* pada perangkat Router Mikrotik RB941.
2. Mengetahui hasil yang didapat setelah di lakukan berbagai pengujian serangan.

1.5 Manfaat Penelitian

Beberapa manfaat yang di dapat dari penelitian ini :

1. Meningkatkan keamanan jaringan pada perangkat router mikrotik.
2. Mencegah serangan dari hacker yang ditujukan pada pencurian data akses login dan *port* yang ada pada perangkat router.
3. Sebagai referensi dan acuan dalam menentukan metode keamanan jaringan.

1.6 Sistematika Penulisan

Sistematika penulisan yang dibuat untuk mempermudah pemahaman terhadap skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi tinjauan pustaka, dan dasar-dasar teori yang digunakan dalam penelitian ini.

BAB III METODE PENELITIAN

Pada bab ini didalamnya terdapat tinjauan umum tentang objek penelitian, analisis masalah, solusi yang ditawarkan, dan rancangan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini merupakan tahapan yang penulis lakukan dalam mengembangkan sistem keamanan, testing hingga penerapan pada objek penelitian.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian.