

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada zaman sekarang teknologi berkembang dengan sangat pesat dan mengarah ke era digitalisasi. Keamanan jaringan suatu institusi merupakan salah satu urgensi yang harus diperhatikan dalam menjaga integritas dan validitas data. Untuk memastikan bahwa layanan selalu tersedia bagi pengguna. Sistem yang digunakan untuk mendeteksi penyusup jaringan di era 4.0 umumnya sudah mampu mendeteksi berbagai jenis namun belum dapat melakukan tindakan pencegahan, namun dari sisi pengguna, pengguna memang membutuhkan teknologi informasi yang menjadi salah satu penyebab penyusup. Kasus keamanan di Indonesia, jumlah jaringan di mana hal ini terjadi meningkat setiap tahun karena rendahnya tingkat kekhawatiran keamanan siber oleh organisasi. Oleh karena itu, dibutuhkan sebuah system yang mampu mempermudah administrator jaringan untuk memonitoring traffic jaringan. Tidak hanya sistem keamanan jaringan yang harus ditingkatkan tetapi kesadaran diri atau awareness dalam menjaga data-data penting harus diperhatikan[1].

Hal ini dapat dibuktikan ketika dilakukan scanning port, terlihat bahwa service port untuk melakukan remote akses pada router mikrotik dalam status port. Hampir sebagian serangan keamanan jaringan dilakukan dengan cara mengetahui informasi terhadap port-port yang terbuka kemudian dilakukan exploit. Usaha pencegahan yang dapat dilakukan untuk pengamanan pada service port yaitu dengan melakukan blocking port menggunakan firewall. Akses terhadap port tetap bisa dilakukan melalui pemanfaatan metode port knocking. Port knocking merupakan metode untuk mengakses port yang telah diblok dengan mengirimkan packet atau koneksi sesuai dengan aturan knocking yang telah dibuat[1].

1.2 Rumusan Masalah

Berdasar latar belakang masalah diatas maka rumusan masalahnya sebagai berikut :

1. Bagaimana perbandingan Mikrotik yang menggunakan metode *firewall filtering* dan *port knocking* dengan yang tidak menggunakan?
2. Apakah kinerja sistem keamanan jaringan terhadap serangan DDoS, Port Scanning, dan Sniffing mengalami penurunan?

1.3 Batasan Masalah

Penelitian yang dilakukan memiliki batasan masalah, dimana hal ini digunakan untuk memudahkan penulis dalam proses pencarian data, literatur, dan juga pengerjaan. Batasan-batasan tersebut ialah:

1. Parameter yang digunakan untuk mengukur keamanan jaringan adalah DDoS, Port Scanning, dan Sniffing.
2. Port yang digunakan pada penelitian ini yaitu port 80 dan port 8291
3. Hanya membahas tentang keamanan jaringan pada perangkat Mikrotik RB951Ui-2HND dengan menggunakan firewall filter dan port knocking sebagai rules pengamanannya.

1.4 Tujuan Penelitian

Tujuan penelitian ini berisi tentang membandingkan dan meningkatkan keamanan jaringan dengan menerapkan metode *firewall filtering* dan *port knocking* supaya sistem dapat mendeteksi serangan berbahaya.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberi ilmu dan pemahaman lebih lanjut mengenai keamanan jaringan dan dapat menjadi acuan maupun rujukan bagi perusahaan maupun instansi yang menggunakan metode firewall filtering dan port knocking.

1.6 Sistematika Penulisan

Berisi sistematika penulisan skripsi yang memuat uraian secara garis besar isi skripsi untuk tiap-tiap bab. Peneliti harus dapat mendeskripsikan (menggambarkan) apa saja isi masing-masing Bab yang akan disusun. Jelaskan secara singkat isi dari bab I, bab II, bab III, bab IV, dan bab V.

Contoh :

BAB I PENDAHULUAN, berisi Latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, dan penulisan sistematika penelitian

BAB II TINJAUAN PUSTAKA, berisi tinjauan pustaka, dasar-dasar teori yang digunakan untuk mendukung penulisan penelitian ini

BAB III METODE PENELITIAN, didalamnya terdapat tinjauan umum tentang objek penelitian, analisis masalah, solusi yang ditawarkan, diagram alur perancangan system, spesifikasi alat dan bahan.

BAB IV HASIL DAN PEMBAHASAN, pada bab ini berisi tentang implementasi, uji coba pengujian, dan hasil dari penelitian ini.

BAB V PENUTUP, bab ini berisi kesimpulan dan saran penulis untuk pengembangan system.