BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan internet merupakan salah satu teknologi yang paling cepat dan memiliki dampak meningkatnya *cyber crime* dengan tingkat yang tinggi. Keamanan jaringan secara umum jika sebuah komputer yang terhubung ke sebuah jaringan maka akan lebih berpotensi terserang berbagai ancaman keamanan dibandingkan komputer yang tidak terkoneksi ke jaringan (Garfinkel, Spafford, 2018). Keamanan jaringan yang mampu untuk mengantisipasi ancaman di dalam jaringan komputer baik dari ancaman sistem maupun fisik. Ancaman sistem yang dimaksud adalah berupa penyusupan,pencurian data, maupun tindakan *hacking* pada sistem sedangkan ancaman fisik yaitu yang merusak fisik atau *hardware* perangkat.

Cimun Net merupakan sebuah *internet café* skala *mikro* yang beralamat di Jl. Kp. Lamaran No.6, Palumbonsari, Kec. Karawang Timur, Kabupaten Karawang, yang bergerak di bidang jasa, bidang jasa usaha ini berfokus pada jasa layanan *internet* yang bervariasi masa waktunya yaitu bisa berupa hitungan jam, hari, maupun bulanan.

Setiap keamanan pasti mempunyai beberapa kelemahan, termasuk pada keamanan jaringan komputer. Keamanan jaringan komputer merupakan proses pencegahan dan identifikasi terhadap penggunaan hak akses pada jaringan yang bertujuan untuk mencegah pihak yang tidak memiliki otorisasi agar tidak bisa mengakses jaringan komputer. Kewaspadaan tersebut tentu harus diiringi dengan kemampuan pengelola jaringan komputer agar bisa meningkatkan keamanan jaringan komputer dari pihak yang akan melakukan *hacking*.

Jaringan komputer mempunyai berbagai macam metode keamanan, *port knocking* merupakan sebuah metode yang memungkinkan untuk membuka akses menuju perangkat jaringan melewati *port* tertentu yang akan diproses oleh *firewall* dengan cara mengirimkan koneksi atau paket yang berupa protocol ICMP, UDP, TCP ke perangkat jaringan sehingga pada saat ingin mengakses harus melewati *port* yang telah ditentukan terlebih dahulu. *Port knocking* bisa untuk membantu pencegahan terhadap proses *scanning* yang bertujuan untuk mengeksploitasi layanan *port* yang tersedia pada perangkat yang juga berfungsi sebagai *firewall* terhadap serangan *zero-*

day (Sel,Totakura, Carle, 2018).

Lebih lanjut untuk memudahkan administrator jaringan agar bisa memantau perangkat jaringan yaitu *router* Mikrotik yaitu dengan mengirimkan notifikasi berupa pesan melalui aplikasi Telegram apabila terjadi serangan pada *router* yang berupa tindakan mencoba login berulang kali.

Berdasarkan uraian diatas maka dibuatlah penelitian dengan judul yang relevan menggunakan latar belakang penelitian ini adalah "Penerapan Metode *Port Knocking* Pada Sistem Keamanan Jaringan Berbasis Notifikasi Telegram"

1.2. Rumusan Masalah

1. Bagaimana cara mengimplementasikan metode *port knocking* pada sistem keamanan jaringan komputer di Cimun Net ?
2. Bagaimana cara mendeteksi serangan pada mikrotik, lalu mengirim notifikasi pesan melaui aplikasi telegram ?

1.3. Tujuan Penelitian

1. Mengetahui cara mengimplementasikan metode *Port Knocking* pada sistem keamanan jaringan komputer di Cimun Net.
2. Bagaimana mengetahui adanya serangan pada mikrotik, lalu mengirimkan notifikasi lewat aplikasi telegram.

1.4. Manfaat

Manfaat penelitian ini bertujuan agar sebagai sumber pengetahuan dan informasi terhadap keamanan jaringan dan melakukan pengamanan sehingga dapat mengirimkan notifikasi langsung ke *administrator* jaringan secara *realtime*.