BAB 1
PENDAHULUAN

1.1 Latar Belakang

Semakin meningkatnya perkembangan teknologi Internet maka *cyber crime* juga akan meningkat. Pada kebutuhan untuk meningkatkan keamanan jaringan komputer di era digital saat ini. banyak organisasi dan perusahaan harus memperhatikan keamanan jaringan mereka agar tidak terjadi kebocoran data dan kerugian finansial yang besar. Pada jurnal Computer Law & Security Review menjelaskan *cyber crime* adalah mengacu pada serangkaian tindakan kriminal yang dilakukan dengan menggunakan atau melibatkan teknologi komputer dan jaringan elektronik. Tindakan-tindakan ini melibatkan penggunaan komputer, perangkat lunak, internet, dan sistem jaringan lainnya untuk melakukan kegiatan ilegal atau merugikan. Kejahatan siber bisa mencakup berbagai jenis tindakan, termasuk pencurian data pribadi, pencurian identitas, penipuan daring, serangan siber, perusakan data, penyebaran malware, dan banyak lagi (Porcedda, 2023).Kejahatan siber dapat menyasar individu, perusahaan, pemerintah, atau institusi lainnya. Tujuan dari tindakan ini bisa bervariasi, termasuk mendapatkan keuntungan finansial, merusak reputasi, mencuri informasi rahasia, atau bahkan melakukan tindakan sabotase. Dalam beberapa kasus, kejahatan siber juga dapat memiliki dampak yang luas dan serius, termasuk ancaman terhadap keamanan nasional.

Mikrotik merupakan salah satu perangkat jaringan yang banyak digunakan oleh organisasi dan perusahaan untuk mengatur jaringan komputer. Namun, meskipun *Mikrotik* sudah dilengkapi dengan berbagai fitur keamanan, tidak menjamin bahwa jaringan yang dibangun di atasnya terbebas dari serangan(Sumardi & Zaen, 2018). *MikroTik RouterOS* merupakan sistem operasi yang fleksibel dan dapat digunakan untuk berbagai jenis jaringan, mulai dari jaringan kecil hingga jaringan besar yang kompleks. *RouterOS* dilengkapi dengan berbagai fitur, seperti routing statis dan dinamis, *firewall, QoS, hotspot, VPN*, dan banyak lagi. Selain itu, *RouterOS* dapat diinstal pada perangkat keras *MikroTik* yang berbeda, seperti *router, switch*, dan *access point*, yang memberikan fleksibilitas dalam merancang dan mengelola jaringan.

Serangan *cyber crime* bisa diartikan kejahatan yang terjadi di internet dan dilakukan oleh pelaku dengan mencari kelemahan sebuah jaringan internet(Gultom, 2022). Pelaku serangan *cyber* juga sering disebut dengan hacker, Menurut Dr. Sunil Kumar Assistant Professor, *Dept of Computer Science* Sangam University, Bhilwara, Rajasthan di jurnal yang berjudul *Hacking Attacks, Methods, Techniques And Their Protection Measures*, *Hacking* adalah kegiatan merusak, mengambil, mengubah sebuah program dan mengambil data penting tanpa izin. Pelaku dari peretasan ini disebut *Hacker*, *Hacker* bisa berkelompok maupun individu(Kumar & Agarwal, 2018).

Ada beberapa jenis serangan yang bisa terjadi pada suatu jaringan contohnya adalah DDoS, *Man-in-the-Middle Attack*, dan *Unautorized Access*, Serangan DDoS bekerja dengan cara mengganggu *Network Traffic* sehing menyebabkan *server down*(Ridho & Arman, 2020). *Man in the Middle Attac*k (MITM) adalah jenis serangan pada jaringan komputer yang dilakukan dengan cara memanipulasi koneksi antara dua pihak yang sedang berkomunikasi secara langsung. Pada serangan ini, penyerang dapat memasukkan dirinya di tengah-tengah komunikasi dan menerima, merekam, bahkan memodifikasi informasi yang dikirimkan antara dua pihak tersebut(Mallik et al., 2019). Kemudian ada juga jenis serangan *Unautirized Access* adalah ketika seseorang atau pihak yang tidak memiliki hak atau izin untuk mengakses sistem atau data tertentu berhasil memperoleh akses. Hal ini dapat terjadi ketika seseorang berhasil menebak atau mencuri username dan password, mengambil alih akun orang lain, atau mengeksploitasi kerentanan sistem yang ada(AbdAllah et al., 2018). Maka dari itu keamanan jaringan perlu ditingkatkan lagi untuk menerapkan internet aman dan sehat maka perlu keamanan jaringan yang bagus.

Ada beberapa jenis keamanan jaringan yang bisa digunakan untuk mengamankan sebuah jaringan, Contohnya seperti *HoneyPot*, *Point To Point Tunneling Protocol* dan *Port Knocking* . Dalam penelitian ini menggunakan keamanan jaringan *Port Knocking*. *Port Knocking* adalah jenis keamanan yang bekerja dengan cara

menyembunyikan layanan jarak jauh di *firewall*, memungkinkan akses ke port tersebut hanya untuk informasi tentang layanan setelah klien berhasil mengautentikasi ke *firewall*. Ini dapat membantu mencegah pemindai mengetahui layanan apa yang saat ini tersedia di host dan juga berfungsi sebagai pertahanan terhadap serangan zero-day(Sel et al., 2016). Secara sederhana, *port knocking* mengharuskan pengguna untuk melakukan serangkaian koneksi ke port-port tertentu secara berurutan dalam waktu yang singkat dan dengan pola tertentu. Pola ini kemudian diidentifikasi oleh server yang menjalankan firewall, yang kemudian membuka port-port tertentu untuk pengguna yang telah memenuhi syarat. Setelah pengguna selesai menggunakan port tersebut, port-port tersebut akan otomatis ditutup kembali. Dengan menggunakan teknik *port knocking*, akses ke port-port yang sensitif dan rawan serangan dapat diatur dengan lebih aman dan efektif, karena hanya pengguna yang telah melewati tahap autentikasi yang tepat yang dapat mengakses port tersebut. Teknik ini juga dapat membantu mencegah serangan *brute force* dan mengurangi jumlah log yang dibuat oleh firewall, karena hanya permintaan koneksi yang sah yang akan dicatat.

Menurut jurnal yang berjudul "*Digital Certificate-based Port Knocking for Connected Embedded Systems"* yang ditulis oleh Basim Mahbooba dan Michael Schutat menjelaskan Port knocking (PK), juga disebut sebagai spread-spectrum TCP, adalah sebuah cara untuk meningkatkan ketahanan komputer yang terhubung dalam

jaringan terhadap serangan siber. Dalam bentuk paling dasarnya, metode ini melibatkan pengiriman paket UDP atau TCP oleh klien ke berbagai port server dalam urutan yang telah ditentukan sebelumnya untuk memberikan akses ke server tersebut(Mahbooba & Schukat, 2017). Urutan port knocking hanya diketahui oleh entitas yang memiliki otorisasi . Secara teknis, PK menutup semua port pada perangkat jaringan melalui firewall. Firewall hanya akan memberikan akses ke port tertentu (misalnya, mengizinkan paket jaringan dari sumber tertentu untuk melewati firewall) jika klien menyajikan "rahasia" bersama kepada firewall penerima melalui pengiriman serangkaian paket yang mengandung "rahasia" tersebut.

Untuk melakukan perancangan jaringan di penelitian ini menggunakan software simulasi GNS3. Dalam simulasi GNS3, kita dapat merancang jaringan virtual yang terdiri dari berbagai perangkat Mikrotik yang terhubung satu sama lain. GNS3 (Graphical Network Simulator-3) adalah perangkat lunak simulasi jaringan yang memungkinkan pengguna untuk merancang, menguji, dan mengimplementasikan jaringan virtual yang kompleks menggunakan topologi jaringan yang berbeda. (DAYANAND LAL N et al., 2016). GNS3 sangat berguna untuk para profesional jaringan, mahasiswa, dan penggemar teknologi yang ingin menguji konfigurasi jaringan yang kompleks dan memahami cara kerja jaringan secara lebih mendalam. Dalam hal ini, GNS3 adalah salah

satu perangkat lunak simulasi jaringan yang paling populer dan sering digunakan.

Dengan demikian, berdasarkan uraian di atas perancangan keamanan jaringan pada Mikrotik menggunakan simulasi GNS3 dengan metode *port knocking* menjadi penting untuk meningkatkan keamanan jaringan dan melindungi data dari ancaman yang tidak diinginkan.

1.2 Rumusan Masalah

1. Bagaimana cara membuat perancangan keamanan jaringan dengan menggunakan Metode *Port Knocking*?
2. Bagaimana cara memantau dan mengawasi jaringan untuk mendeteksi aktivitas yang mencurigakan atau ancaman keamanan potensial ?
3. Bagaimana cara mengkonfigurasi metode port knocking dalam merancang sistem keamanan jaringan MikroTik menggunakan simulasi GNS3?

1.3 Batasan Masalah

Berdasarkan judul tersebut, berikut adalah beberapa batasan masalah yang dapat dijabarkan

1. Fokus penelitian pada perancangan keamanan jaringan pada perangkat Mikrotik menggunakan metode *Port Knocking* dengan simulasi GNS3.

2. Penelitian hanya membahas mengenai implementasi metode *Port Knocking* pada Mikrotik menggunakan GNS3, bukan pada perangkat nyata.
3. Analisis keamanan akan dilakukan dengan menguji efektivitas metode *Port Knocking* dalam mengamankan jaringan pada Mikrotik.
4. Penelitian tidak membahas aspek perancangan jaringan Mikrotik secara keseluruhan, namun hanya berfokus pada aspek keamanan jaringan.
5. Penelitian tidak membahas implementasi metode keamanan lainnya pada Mikrotik selain *Port Knocking*.

1.4 Tujuan Penelitian

1. Membuat Design keamanan jaringan dengan menggunakan aplikasi simulasi jaringan GNS3
2. Menggunakan teknologi keamanan jaringan seperti firewall, VPN, dan teknologi keamanan lainnya dapat membantu dalam mendeteksi aktivitas yang mencurigakan dan mencegah serangan keamanan.
3. Melakukan konfigurasi Port Knocking pada Mikrotik.

1.5 Manfaat Penelitian

1. Penelitian ini dapat membantu meningkatkan keamanan jaringan dengan mengimplementasikan metode *Port Knocking* pada router Mikrotik, sehingga akses ke jaringan

hanya bisa dilakukan oleh orang yang memiliki kunci atau rangkaian kunci tertentu.

2. Dengan menerapkan metode *Port Knocking* pada jaringan Mikrotik, risiko keamanan dapat dikurangi karena hanya pengguna yang memiliki hak akses yang dapat melakukan koneksi ke jaringan.
3. Penelitian ini dapat memberikan pengetahuan dan pengalaman baru dalam penggunaan metode *Port Knocking* pada jaringan Mikrotik, serta dalam penggunaan simulasi virtual machine GNS3