BAB I PENDAHULUAN

1.1. Latar Belakang Penelitian

Keamanan pada jaringan komputer merupakan hal yang penting untuk diperhatikan. Dengan memperhatikan keamanan pada jaringan komputer dapat mencegah serangan-serangan yang datang. Belakangan ini cara untuk melakukan percobaan penyerangan lebih dipermudah dengan adanya *smartphone*. Menggunakan *smartphone* seorang penyerang dapat melakukan observasi, menggunakan terminal, mengakses *database* dari jarak jauh, menggunakan *File Transfer Protocol (FTP)*, dan lain sebagainya. Oleh karena itu, *smartphone* dapat dikatakan mendekati sistem operasi *linux* yang dipasang di *desktop* pada umumnya (*A New Trend of DDoS Attacks: Mobile Devices Are Becoming a New Generation of Botnets - Alibaba Cloud Community*, n.d.; Husain, 2022a). Hal ini membuat jaringan komputer dapat diakses dengan mudah melalui *smartphone*. Dengan demikian diperlukan suatu metode untuk mencegah atau meminimalisasi dampak dari terjadinya penyerangan, dengan cara meningkatkan keamanan untuk mengantisipasi masalah yang akan dihadapi.

Salah satu jenis serangan yang dapat mengganggu fungsi kerja *router* melalui cara *Distributed Denial-of-Service* (*DDoS*). Agar bekerja lebih kuat, *DDoS* biasanya memanfaatkan *Botnet*. *Botnet* adalah kumpulan dari beberapa perangkat seperti komputer, *smartphone*, hingga *IoT* yang terinfeksi dan saling terhubung pada suatu jaringan (Husain, 2022b). Proses penyerangan *Botnet* akan mengakibatkan perangkat terinfeksi. Proses infeksi ini dapat melalui sistem operasi bajakan, mengunduh berkas sembarangan, memasang aplikasi yang berpotensi menjadikannya sebagai *bot*, atau dapat melalui *usb* yang terhubung pada jaringan, sehingga serangan terjadi secara terdistribusi (Peng et al., 2007).

Telah disebutkan bahwa *Internet of Things* (*IoT)* dapat menjadi *Botnet*, walaupun kekuatannya kecil, akan tetapi jika dibiarkan saja lalu menjadi masif, akan menjadi ancaman bagi sistem (Kolias et al., 2017). Melalui penyerangan inilah dapat membebani kerja *router* maupun *server*, sehingga sumber daya seperti *CPU*, kapasitas internet, hingga ruang pada protokol jaringan tersebut tidak dapat digunakan secara maksimal (Mirkovic & Reiher, 2004; Peng et al., 2007). Salah

satu jalan untuk membebani kerja *router* dapat dilakukan dengan cara mengirim terlalu banyak permintaan, membanjiri lalu-lintas dengan banyak data secara berlebihan hingga akhirnya sumber daya *router* atau *server* habis, bahkan dapat mengirim paket cacat atau korup yang dapat membuat protokol atau sistem pada target serangan terpaksa melakukan *booting* ulang atau *hang* (Anthi et al., 2021; Jaya et al., 2020; Mirkovic & Reiher, 2004; Osanaiye et al., 2016; Parusa, 2021).

Berbagai penelitian yang membahas keamanan siber atau yang berhubungan dengan pengelolaan jaringan komputer telah banyak dilakukan, seperti *bandwidth management*, *QOS*, dan *Load Balancing*, akan tetapi rekam jejak terhadap analisis metode penolakan dalam jaringan ini sekilas kurang banyak ditulis. Dengan ditulisnya penelitian ini diharapkan dapat mengungkap celah-celah yang dapat dihindari atau diperbaiki, serta mendapatkan kesimpulan mengenai metode mana yang lebih baik digunakan untuk menangani serangan pada jaringan komputer.

Berdasarkan beberapa kasus yang telah disebutkan di atas, maka perlu untuk mengetahui metode apa yang lebih baik digunakan pada suatu kasus tertentu. Sistem ini akan menggunakan *Firewall* Mikrotik untuk mendeteksi serangan siber, lalu setelah dideteksi akan diterapkan jenis metode yang telah disebutkan yaitu metode *Drop*, *Reject*, *Tarpit*, dan *redirect*. Oleh karena itu, judul yang diambil adalah "ANALISIS METODE PENGAMANAN PADA PENGGUNAAN *FIREWALL* MIKROTIK UNTUK KEAMANAN JARINGAN KOMPUTER".

1.2. Rumusan Masalah

Berdasarkan latar belakang, rumusan masalah yang akan dibahas dalam penelitian ini yaitu:

1. Bagaimana pengamanan jaringan komputer menggunakan metode *Filter Drop*, *Reject*, *Tarpit*, dan *Raw Drop*?
2. Bagaimana pengamanan jaringan komputer dengan algoritma menarik perhatian penyerang melalui *honeypot*?

1.3. Tujuan Penelitian

Tujuan penelitian ini adalah untuk mendapatkan suatu metode yang terbaik pada kasus penolakan *request* di jaringan komputer. Adapun rincian-rincian tujuan lain dalam penelitian ini, adalah sebagai berikut:

1. Untuk mengetahui kekurangan dan kelebihan serta penggunaan *resource* dari metode *Filter Drop*, Reject, *Tarpit*, dan *Raw Drop.*
2. Untuk mengetahui kekurangan dan kelebihan serta penggunaan *resource* dari metode beberapa model *honeypot.*

1.4. Batasan Masalah

1. Percobaan ini dibatasi pada penetrasi melalui *Flood Attack*.
2. Konten menggunakan Mikrotik versi 7.9 dengan kondisi minimum konfigurasi.
3. Metode yang diamati adalah *Drop, Reject, Tarpit*, dan *redirect* ke *honeypot*.
4. Percobaan dilakukan pada jaringan lokal.

1.5. Manfaat Penelitian

Manfaat yang akan didapatkan dari penelitian skripsi ini yaitu:

1. Sebagai referensi untuk menentukan metode yang cocok digunakan dalam menangani keamanan jaringan komputer.
2. Sebagai referensi untuk percobaan penetrasi terhadap sistem yang dibuat.

1.6. Struktur Organisasi

Skripsi ini terbagi menjadi 5 (lima) bab. Bab I menjelaskan mengenai apa yang mendasari penelitian ini dilakukan, dijelaskan pada latar belakang. Selanjutnya adalah mencari tahu apa saja yang akan menjadi topik pembahasan yang akan dibahas pada penelitian ini, berada pada rumusan masalah. Lalu pada sub bab selanjutnya, akan dipaparkan tujuan dan manfaat dari penelitian ini. Pada Bab II berisi tentang tinjauan pustaka, menjelaskan teori-teori yang terhubung dengan penelitian sebelumnya, atau perbandingan penelitian-penelitian yang terkait dengan topik ini. Bab III akan memuat metode yang digunakan dalam penelitian ini. Bab IV mengemukakan temuan dan pembahasan berdasarkan yang telah dilakukan di Bab III. Terakhir, Bab V merupakan bab yang akan memuat kesimpulan dari serangkaian langkah-langkah yang telah ditempuh pada penelitian ini, serta mengandung implikasi dan rekomendasi.