BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan Komputer merupakan sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi. Saat ini jaringan komputer bukan merupakan hal yang baru. Setiap instansi, telah memanfaatkan jaringan komputer. Penggunaan jaringan komputer menjadi sangat meningkat dikarenakan kebutuhan akan informasi yang menjadi semakin tinggi (Pamungkas, 2016). Pemanfaatan teknologi jaringan komputer sebagai media komunikasi data hingga saat ini semakin meningkat.Kebutuhan atas penggunaan berserta *resource* yang ada dalam jaringan baik *software* maupun *hardware* telah mengakibatkan timbulnya berbagai pengembangan teknologi jaringan tersebut. Dengan semakin tingginya kebutuhan dan banyaknya penggunaan jaringan yang menginginkan suatu bentuk jaringan yang dapat memberikan hasil maksimal baik dari segi efisiensi maupun peningkatan keamanan jaringan. Dengan menggunakan sistem operasi router yaitu MikroTik yang menyediakan berbagai fasilitas yang mendukung keamanan dan akses data jaringan (Idrus, 2016).

Keamanan jaringan merupakan salah satu proses untuk mencegah dan memonitoring penggunaan jaringan yang tidak sah dari jaringan komputer. Tujuannya yaitu untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun *logic* baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer (Asep Fauzi Mutaqin, 2016).

Jaringan komputer sangat sensitif karena hanya diberikan melalui server DHCP. Hal tersebut sangat rawan dengan penipuan DHCP. DHCP Rogue Server atau Server palsu dapat memberikan alamat gateway yang tidak benar kekomputer Client, mencegah komputer terhubung ke jaringan atau Internet. Keamanan jaringan yang kurang didukung sering menyebabkan masalah dengan akses Internet di dalam jaringan, karena serangan terhadap server DHCP dilakukan oleh orang yang salah (Kristen *et al.*, 2022).

Sistem *Monitoring* Jaringan merupakan sistem yang berfungsi untuk memantau aktivitas pada perangkat jaringan. Pada penelitian ini, *monitoring* digunakan untuk mengetahui perangkat jaringan mana yang mati dan hidup. Sistem monitoring digunakan untuk memantau, mengawasi, dan mengontrol jalan atau tidaknya suatu perangkat jaringan. Pentingnya monitoring adalah terpantau secara rutin perangkat yang bermasalah yang berpotensi mengganggu jaringan internet (Husna and Rosyani, 2021).

Apabila terjadi masalah pada sebuah perangkat jaringan, sering tidak diketahui secara langsung oleh teknisi jaringan. Alarm ataupun monitoring perangkat jaringan sangatlah penting untuk mengetahui permasalahan atau *trouble* yang terjadi dalam satu jaringan. Jika terjadi *trouble* yang tidak diinginkan, yaitu seperti *accesspoint - accesspoint* yang digunakan untuk mengatur akses yang ada di suatu perangkat jaringan berdasarkan MAC address. teknisi jaringan tidak dapat langsung mengambil tindakan perbaikan yang cepat, sehingga membutuhkan banyak waktu untuk menganalisa dan penyelesaian terhadap permasalahan yang terjadi demi kelancaran dan kembali normalnya akses internet. *Administrator* jaringan menggunakan *Router mikrotik* sebagai pengatur jaringan lokal yang belum

memanfaatkan *netwatch* dimana melalui fitur tersebut *Administrator* jaringan dapat melakukan monitoring terhadap kondisi sebuah perangkat atau *accesspoint* yang bisa diintegrasikan dengan aplikasi telegram (Havest, 2020).

Salah satu pemanfaatan keamanan pada mekanisme konfigurasi alamat jaringan menggunakan DHCP, Rogue DHCP *server* memberikan konfigurasi alamat jaringan yang salah kepada client yang tergabung di dalam jaringan dengan tujuan menciptakan serangan berupa man-in-the-middle, apabila terdapat DHCP Rogue server pada perangkat jaringan, dapat menyebabkan beberapa permasalahan, di antaranya bisa menyebabkan konflik IP di suatu perangkat jaringan atau Client mendapatkan *Default Gateway* yang tidak sesuai sehingga perangkat Client tidak bisa mengakses internet.

Solusi dari permasalahan diatas supaya lebih mempermudah *Network Administrator System* dalam monitoring sebuah host *Up/Down* atau *accesspoint* dan mencegah serangan DHCP *Rogue* pada jaringan, maka penulis memberikan usulan untuk membuat suatu sistem monitoring jaringan. Untuk melakukan monitoring perangkat jaringan, penulis memanfaatkan fitur *netwatch* pada mikrotik untuk menjalankan script yang akan mengirimkan notifikasi ke telegram, sedangkan untuk monitoring serangan DHCP Rogue, penulis memanfaatkan fitur DHCP *Alert*, fitur ini dapat menjalankan script secara otomatis ketika ada DHCP tandingan atau serangan DHCP Rogue, sehingga router dapat mengirimkan *Alert* ke telegram.

Berdasarkan uraian diatas, maka penulis tertarik untuk melakukan penelitian dengan judul**: "Implementasi Sistem Monitoring Jaringan Menggunakan**

Mikrotik dan DHCP *Alert* Untuk Mencegah Serangan DHCP Rogue Dengan Notifikasi Bot Telegram".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan diatas, maka penulis dapat merumuskan beberapa masalah yang ingin dijawab dalam penelitian ini. Yaitu sebagai berikut:

1. Bagaimana merancang sistem *monitoring* menggunakan mikrotik dan Dhcp *Alert* mencegah serangan dhcp Rogue dengan notifikasi telegram?
2. Bagaimana sistem yang dibuat ini nantinya bisa memantau beberapa device yang up dan down secara *real time*?
3. Bagaimana merancang sistem monitoring berbasis dengan sistem *Alert* Telegram?

1.3 Batasan Masalah

Berikut adalah Batasan masalah dalam penelitian yang dilakukan:

1. Mikrotik yang digunakan dalam pengujian menggunakan Mikrotik RB941.
2. Pengujian Up/Down perangkat dilakukan dengan mematikan mematikan perangkat kemudian dihidupkan Kembali untuk mentrigger script yang telah dibuat
3. Pengujian DHCP Rogue dilakukan dengan memanfaatkan router lain untuk membuat DHCP Tandingan.
4. Sistem monitoring up/down perangkat menggunakan fitur *netwatch* yang ada pada mikrotik untuk menjalankan script.

5. Sistem monitoring serangan DHCP Rogue menggunakan fitur DHCP *Alert* yang ada pada mikrotik untuk menjalankan script.
6. Bot Telegram dibuat menggunakan fitur BotFather.

1.4 Tujuan Penelitian

Tujuan umum dari penelitian ini adalah melakukan implementasi sebuah sistem keamanan jaringan yang dapat memonitor kapan perangkat server sedang up atau down pada perangkat-perangkat, dan Dhcp Alert dapat mencegah serangan Dhcp Rogue dengan Notifikasi Bot Telegram, dengan memanfaatkan tools Netwatch yang ada pada mikrotik untuk dapat melihat gambaran dan informasi mengenai lalu lintas data jaringan yang terjadi pada setiap perangkat, serta memberikan informasi lebih cepat kepada *Network administrator* bila terjadi masalah pada setiap perangkat jaringan.

1.5 Manfaat Penelitian

Manfaat yang diharapkan pada penelitian ini antara lain:

1. Dapat membantu Network administrator dalam upaya monitoring perangkat jaringan secara cepat.
2. Lebih hemat biaya dan waktu untuk *maintenance.*
3. Dapat mengidentifikasi dan mengatasi masalah secepat mungkin sebelum mendapat complain.