

# BAB 1

## PENDAHULUAN

### 1.1 Latar Belakang

Perkembangan teknologi yang pesat saat ini, memegang peranan yang sangat penting sehingga, keamanan informasi menjadi prioritas utama. Dengan begitu cepatnya perkembangan teknologi jaringan komputer saat ini, banyak hal yang harus di perhatikan oleh pengelola jaringan yaitu keamanan jaringan itu sendiri. Di era sekarang jaringan komputer banyak digunakan bahkan hampir semua orang termasuk para *hacker* atau pun *cracker*. Adapun tujuan para *hacker* dan *cracker* melakukan peretasan melalui port-port yang ada pada jaringan adalah untuk menyalin data, mengambil data, bahkan sampai mengacak-acak data. Hal ini dapat merugikan pemilik server. Banyak organisasi saat ini yang menggunakan jaringan komputer untuk melakukan pertukaran informasi data, baik itu organisasi komersial (perusahaan), lembaga pemerintah, dan perguruan tinggi. Dengan meningkatkan sistem keamanan jaringan dapat mengurangi bahkan mencegah dari ancaman ataupun serangan dari para *hacker* dan *cracker*. Saat ini CV Dizam Network Solusion sedang mengalami masalah seperti diatas yaitu perangkat router mikrotik yang digunakan untuk jalur *backbone* sering di akses oleh user yang tidak di ketahui sehingga sering terjadinya perubahan settingan pada perangkat router mikrotik dan bahkan pernah sampai penghapusan settingan. Oleh karena itu penulis ingin merancang bangun system keamanan jaringan komputer dengan menggunakan metode port knocking pada CV Dizam Network Solusion

Sistem keamanan jaringan merupakan proses pencegahan ataupun melakukan identifikasi para pengguna yang tidak diizinkan dari jaringan komputer. Ada beberapa cara untuk meningkatkan keamanan jaringan, salah satunya dengan cara menerapkan metode port knocking pada sistem jaringan[1].

Pesatnya perkembangan teknologi internet tidak bisa disangkal bahwa hal ini akan mempengaruhi peningkatan kejahatan dunia maya (*Cyber Criem*). Oleh karena itu kita sebagai pengguna (*user*) harus berhati-hati dalam menggunakan jaringan komputer. Berikut ini adalah serangan yang bisa saja terjadi saat menggunakan jaringan komputer, *Denial of Service (DoS)*, *Smurf Attack*, *Wirllless*

*Attack, DNS Poisoning*. Serangan DoS adalah tindakan yang diambil dengan mengganggu atau merusak jaringan, sistem, atau aplikasi yang menghabiskan sumber daya seperti CPU, memori, bandwidth, dan hardisk[2].

Jaringan komputer tidak akan aman jika tidak di terapkan sistem keamanan. Kerentanan yang sering terjadi pada jaringan komputer yaitu kehilangan-nya *data* atau *file* bahkan *system crash*, karena serangan yang semakin canggih dan beragam. Keamanan jaringan merupakan masalah yang sangat penting untuk diperhatikan terutama ketika jaringan bersifat lokal. Perlunya diterapkan sistem keamanan jaringan pada perangkat router mikrotik dengan menerapkan sistem port knocking[3].

Port knocking adalah metode membuka ataupun menutup akses ke port tertentu kemudian diblokir oleh *firewall* pada perangkat jaringan, dengan mengirimkan paket atau koneksi. Pengguna dapat menggunakan port dengan sesuka hati karena mengetahui hak akses dan cara membuka port yang telah pengguna konfigurasi[4].

Berikut ini adalah beberapa penelitian terdahulu yang pernah dilakukan mengenai perancangan sistem keamanan jaringan menggunakan metode port knocking. Penelitian Abdul Jamalul'ain Odi Nurdiawan Martanto, pada tahun 2022 mengenai "Optimalisasi Keamanan Jaringan Komputer Menggunakan Metode Knocking Port Berbasis Mikrotik"[5]. Penelitian Gunawan Indra Okta Kirana pada tahun 2022. mengenai Optimalisasi Sistem Keamanan Jaringan Komouter Terhadap Serangan Malware Menggunakan Filtering Firewall Dengan Metode Port Knocking. [6] Penelitian Widharma, I Gede Saputra pada tahun 2020 mengenai Pengamanan Sistem Jaringan Komputer Dengan Teknologi Firewall[7]. Penelitian Budi Jaya Yuhandri Yunus Sumijan pada tahun 2020 Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS) [8] Penelitian A. Amarudin pada tahun 2018 mengenai Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking[2].

Router mikrotik berfungsi sebagai media atau alat penghubung antar jaringan, selain itu manfaat router mikrotik sangat banyak salah satunya yaitu memiliki fitur *filter rules* yang dimana berguna untuk melakukan pemblokiran atau membatasi paket data yang masuk sehingga jaringan internet yang di salurkan menjadi lebih

aman[9]. Dengan begitu penulis ingin melakukan perancangan sistem keamanan jaringan computer dengan menggunakan perangkat Mikrotik RB-951UI-2ND yang bertujuan untuk meningkatkan keamanan jaringan pada CV Dizam Network Solusion.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang di atas dapat diambil rumusan masalah dalam tugas akhir ini diantara yaitu:

1. Bagaimana cara meningkatkan keamanan jaringan komputer?
2. Bagaimana mengimplementasikan *port knocking* pada Mikrotik RB951UI-2ND?
3. Bagaimana cara mengakses port router mikrotik yang sudah di konfigurasi menggunakan *port knocking*?

## 1.3 Batasan Masalah

Adapun batasan masalahnya, meliputi:

1. Mikrotik yang digunakan adalah Router Mikrotik RB951UI-2ND
2. Pengguna hanya bisa mengakses port-port yang sudah di tentukan untuk mengaksesnya
3. Pembuatan metode *port knocking* menggunakan protokol ICMP, Telnet, dan SSH
4. Aplikasi yang digunakan untuk pengujian menggunakan PuTTY
5. Sistem pengujian hanya dilakukan di CV Dizam Network Solusion

## 1.4 Tujuan Penelitian

Sesuai dengan rumusan masalah yang ada, penelitian ini bertujuan untuk:

1. Membuat metode *port knocking* dengan protocol ICMP, Telnet, dan SSH yang di pasang pada firewall agar keamanan jaringan lebih baik.
2. Membuat rules terhadap perangkat mikrotik, agar user yang tidak dikenal tidak dapat akses untuk masuk
3. User harus mengikuti rules yang telah ditentukan oleh admin jaringan

## 1.5 Manfaat Penelitian

Manfaat dari tujuan penelitian yang di capai adalah sebagai berikut:

1. Dengan adanya metode *port knocking* ini akan menjadi salah satu cara untuk meningkatkan keamanan jaringan komputer yang ada.
2. Bagi administrator jaringan mereka dapat menentukan siapa saja yang dapat memiliki akses dan memasuki port-port tertentu dengan sesuai ketentuan yang dibuat.
3. Menjamin keamanan jaringan pada CV Dizam Network Solusion tidak mudah untuk di serang

## 1.6 Sistematika Penulisan

Pada sistematik penulisan ini penulis memberikan gambaran umum mengenai penelitian yang dijalankan. Sistematika penulisan penelitian sebagai berikut:

### **BAB I PENDAHULUAN**

Dalam Bab ini menjelaskan tentang Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Mafaat Penelitian, dan Sistematika Penulisan.

### **BAB II LANDASAN TEORI**

Dalam Bab ini membahas tentang berbagai teori dan konsep yang berkaitan dengan judul yang diambil, supaya berguna disaat proses analisis permasalahan penelitian yang pernah dilakukan sebelumnya.

### **BAB III METODOLOGI PENELITIAN**

Pada Bab ini membahas tentang metodologi penelitian yang digunakan mengenai perancangan dan membangun sistem keamanan jaringgan komputer menggunakan metode port knocking

#### **BAB IV PEMBAHASAN**

Pada Bab Ini menjelaskan rincian hasil yang diperoleh dari penelitian yang dilakukan, dan juga membahas tentang sistem berjalan dan sistem yang diusulkan. Pembahasan tersebut terdiri dari struktur organisasi, tugas dan wewenang, analisis sistem masalah yang berjalan, analisis kebutuhan dari sistem yang diusulkan. *Unified Modelling Language (UML)* yang terdiri dari beberapa diagram antara lain Activity Diagram, Use Case Diagram, dan Deskripsi Use case dan yang terakhir struktur tampilan topologi jaringan.

#### **BAB V PENUTUP**

Dalam Bab ini membahas kesimpulan dan saran yang diperoleh dari materi pembahasan yang dibuat. Pada Bab ini juga berisi kesimpulan yang telah dilaksanakan dalam pemanfaatan Mikrotik RB 951 2ND, dan saran yang diusulkan untuk keamanan sistem agar menghasilkan sistem yang lebih efektif dan efisien

