

## **BAB I**

### **PENDAHULUAN**

#### **1.1 Latar Belakang Masalah**

Pada penelitian sebelumnya yang dilakukan oleh AI Haris, B Riyanto, F Surachman, AA Ramadhan pada tahun 2022. Dengan judul Analisis Pengamanan Jaringan Menggunakan *Router Mikrotik* dari Serangan DoS dan Pengaruhnya Terhadap Performansi. Penelitian ini menjelaskan, *Denial of Service* (DoS) dapat menyebabkan kerusakan parah dengan membanjirinya dengan *traffic* dalam jumlah besar. *Router*, sebagai *gateway* dalam jaringan, mempunyai peran yang sangat penting. Apabila fungsinya terganggu, maka akan berdampak langsung terhadap kinerja jaringan. Oleh karena itu, penelitian ini ingin mengevaluasi efektivitas pengamanan jaringan menggunakan *router Mikrotik* dengan memanfaatkan fitur-fitur keamanan bawaan. Tujuannya ialah untuk menilai tingkat keefektifan sistem keamanan tersebut. Didapatkan hasil yaitu terbukti dari konsumsi CPU berhasil diturunkan hingga 15%, *ping response time* turun kembali ke kondisi normal, dan proses deteksi serta blokir dapat dilakukan oleh firewall raw secara otomatis.(Haris et al., 2022).

Pada penelitian yang dilakukan oleh Yudi Mulyanto, M. Julkarnain, Aldela Jabi Afahar, yang berjudul Implementasi *Port Knocking* untuk Keamanan Jaringan SMKN 1 Sumbawa Besar pada tahun 2021. Pada penelitian ini menjelaskan bahwa metode *port knocking* dalam keamanan jaringan dan agar dapat mencegah serangan pada *port-port* jaringan komputer SMKN 1 Sumbawa Besar. Hasil dari penelitian ini menyatakan bahwa peningkatan keamanan jaringan menggunakan metode *Port*

*Knocking* yang dapat membantu meningkatkan keamanan jaringan dan membantu administrator dalam mengamankan *Mikrotik Routerboard* pada sistem jaringan komputer SMKN 1 Sumbawa Besar. (Yudi mulyanto et al., 2021).

Pada penelitian yang dilakukan oleh Sugeng Riyadi, Jasimir, Yudi Novianto, yang berjudul Perancangan Sistem *Monitoring* Jaringan Internet Pada PT Sepulsa Teknologi Indonesia Berbasis *Mikrotik* pada tahun 2021. Pada penelitian ini menjelaskan bahwa penggunaan *mikrotik* dalam keamanan jaringan dengan membuat sistem pemantauan jaringan yang otomatis dijalankan oleh sistem dan mengirimkan notifikasi melalui *Telegram* dan *E-mail* ketika koneksi dari ISP (*Internet Service Provider*) terputus. Hasil dari proyek ini adalah sebuah sistem yang memudahkan pekerjaan *IT Support* dalam menyelesaikan tugas lainnya serta memantau jaringan menggunakan *Mikrotik*, dengan pengiriman pemberitahuan melalui *E-mail* dan *Telegram*. Dengan sistem ini, pengecekan koneksi *Gateway* secara manual yang biasanya dilakukan tidak lagi diperlukan. (Riyadi & Novianto, 2021).

Pada penelitian yang dilakukan oleh Fauzan Prasetyo Eka Putra, Achmad Zulfikri, Moh Abroril Huda, Hasbullah, Mahendra, Miftahus Surur, yang berjudul Analisis Keamanan Jaringan Dari Serangan *Malware* Menggunakan *Firewall Filtering* Dengan *Port Blocking* pada tahun 2023. Pada penelitian ini menjelaskan bahwa metode *Firewall Filtering* Dengan *Port Blocking* dalam konteks keamanan jaringan, kepentingan untuk mencegah serangan malware yang dapat mengakibatkan kebocoran data, gangguan operasional, dan kerugian finansial yang signifikan.. Hasil dari penelitian ialah untuk memberikan wawasan yang lebih mendalam tentang keamanan jaringan komputer Dengan mengatur *port* di

komputer dan membatasi akses jaringan menggunakan *Mikrotik*, keamanan dan stabilitas jaringan dapat ditingkatkan. Hal ini memungkinkan administrator untuk mengelola *port* yang dibuka atau ditutup, mencegah akses *malware*, dan memberikan perlindungan bagi pengguna yang terhubung. (Zulfikri et al., 2023).

Pada penelitian yang dilakukan oleh Yudi Mulyanto, M. Julkarnain, Aldela Jabi Afahar, yang berjudul Studi kasus keamanan jaringan komputer: analisis ancaman *phising* terhadap layanan *online banking* pada tahun 2022. Pada penelitian ini menjelaskan bahwa ancaman *phising* menyerang berbagai sektor industri, dengan industri perbankan sebagai target utama. Beberapa faktor yang menyebabkan terjadinya *phising* pada layanan perbankan online antara lain adalah kurangnya pengetahuan pengguna, aspek psikologis, dan privasi di media sosial. Penelitian menunjukkan bahwa pencegahan serangan *phising* pada layanan online banking dapat dilakukan melalui beberapa cara, seperti edukasi pengguna, pencegahan *phising* di tingkat *email*, penggunaan perangkat lunak *anti-phising*, serta penerapan sistem OTP dalam perbankan. (Muftiadi et al., 2022).

PT. Rizano Cipta Mandiri Padang merupakan perusahaan yang bergerak dibidang makanan dan minuman. Sebagai sebuah pemasok (distributor) PT. Rizano Cipta Mandiri Padang diwajibkan untuk memiliki koneksi jaringan di perusahaan tetap dalam kondisi yang baik dan lancar karena dapat memengaruhi kinerja perusahaan dalam hal menentukan jumlah persediaan barang yang tepat untuk memenuhi permintaan pasar. Pada saat ini hampir semua perusahaan yang bergerak di bidang industri dihadapkan pada sebuah masalah yaitu adanya risiko keamanan pada jaringan lokal terhadap serangan peretasan oleh pihak yang tidak bertanggung jawab. keamanan siber dapat dibagi menjadi beberapa kategori umum seperti

*network security, information security, dan end-user education.* (Rahmadi & Pratama, 2020). Munculnya risiko keamanan jaringan perusahaan ini memungkinkan adanya celah dalam tiap koneksi *router* dari PT. Rizano Cipta Mandiri dalam menghubungkan semua perangkat di dalam kantor. Jaringan ini memungkinkan karyawan untuk berbagi sumber daya, seperti printer dan file, serta berkomunikasi dengan efisien. Tidak bisa dielakkan bahwa setiap jaringan yang ada pasti memiliki celah yang dapat dimanfaatkan, dan akan selalu ada pihak-pihak yang tidak bertanggung jawab yang berusaha melakukan tindakan yang dapat mengganggu aktivitas jaringan kantor, yang berpotensi menyebabkan kerugian yang signifikan.

*Port Knocking* merupakan salah satu metode *network security* yang dapat digunakan sebagai peningkatan keamanan jaringan pada PT. Rizano Cipta Mandiri. *Port Knocking* adalah metode keamanan jaringan yang memungkinkan akses ke *port* layanan yang tertutup dengan cara menyembunyikan *port* tersebut. Metode ini hanya memberikan akses kepada pengguna yang mengetahui dan mengikuti urutan ketukan yang telah ditentukan. (Amanda et al., 2024). Peneliti menggunakan konsep *Multi-packet Knocking*, yang melibatkan penggunaan beberapa paket yang dikirim dalam urutan tertentu untuk membuka port tertentu. Selain menggunakan metode *Port Knocking*, peningkatan keamanan dapat menggunakan teknik *network security* metode *Port Blocking*. *Port Blocking* adalah menutup semua *port* yang ada, dan hanya pengguna tertentu saja yang dapat mengakses sebuah *port* yang telah ditentukan, yaitu dengan cara mengetuk terlebih dahulu. (Andri et al., 2022). Peneliti menerapkan konsep *Static Port Blocking*, yakni port-port tertentu dapat diblokir oleh administrator jaringan secara manual. Selain menggunakan metode

*Port Knocking* dan *Port Blocking*, peningkatan keamanan yang lebih ketat dapat menggunakan teknik *network security* metode *Firewall Filtering*. *Firewall filtering* adalah teknik yang diusulkan secara tepat waktu beradaptasi dengan kondisi *traffic* menggunakan statistik yang dihitung secara aktif untuk secara dinamis mengoptimalkan urutan aturan penyaringan paket. (Madhloom et al., 2023)

Dari permasalahan tersebut penulis ingin mengangkat judul penelitian yaitu **“PERANCANGAN DAN IMPLEMENTASI NETWORK SECURITY PADA PT. RIZANO CIPTA MANDIRI DENGAN METODE PORT KNOCKING (MULTI-PACKET KNOCKING), STATIC PORT BLOCKING, DAN FIREWALL FILTERING MENGGUNAKAN MIKROTIK ROUTER OS”**.

## 1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas dapat disimpulkan permasalahan yang akan dibahas pada laporan ini sebagai berikut :

1. Bagaimana *Port Knocking* dapat membantu PT. Rizano Cipta Mandiri untuk terhindar dari ancaman peretasan?
2. Bagaimana *Static Port Blocking* dapat membantu PT. Rizano Cipta Mandiri untuk terhindar dari risiko insiden jaringan yang dapat memengaruhi produktivitas dan reputasi perusahaan?
3. Bagaimana penggunaan *firewall filtering* pada *Mikrotik RouterOS*, dapat mengatasi masalah yang dihadapi PT. Rizano Cipta Mandiri dalam implementasi sistem keamanan jaringan?

### **1.3 Hipotesa**

Hipotesa merupakan dugaan sementara dimana nantinya akan dibuktikan dengan hasil penelitian yang dilakukan. Berdasarkan permasalahan yang ada dapat dikemukakan beberapa hipotesa sebagai berikut :

1. Diharapkan dengan implementasi metode keamanan jaringan yang efektif, seperti penggunaan *port knocking*, PT. Rizano Cipta Mandiri dapat mengurangi risiko serangan peretasan dan melindungi data sensitifnya.
2. Diharapkan dengan implementasi metode keamanan jaringan yang efisien, seperti penggunaan *port blocking*, PT. Rizano Cipta Mandiri dapat mengurangi risiko insiden jaringan dan menjaga kontinuitas operasional serta reputasi perusahaan.
3. Diharapkan penggunaan *firewall filtering* pada *Mikrotik Router OS* dapat meningkatkan kemampuan deteksi dan respons terhadap serangan siber di PT. Rizano Cipta Mandiri.

### **1.4 Batasan Masalah**

Untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah dalam penyusunan penelitian ini maka peneliti memberikan batasan masalah yaitu, peneliti hanya menggunakan satu laptop dan satu *mikrotik* untuk membuat *Port Knocking*, *Port Blocking* dan *Firewall Filtering*, yang mungkin tidak cukup untuk menguji keamanan jaringan secara menyeluruh. Keterbatasan dalam keakuratan informasi, seperti alamat IP server dan beberapa perangkat lainnya, disebabkan oleh fakta bahwa informasi tersebut merupakan rahasia perusahaan yang tidak dapat

diungkapkan kepada peneliti. Objek penelitian akan dilakukan pada PT. Rizano Cipta Mandiri, perancangan yang akan dibuat nantinya akan diimplementasikan ke perangkat *Mikrotik* dengan sistem operasi *Router OS* dan diuji coba dengan menggunakan *software Putty*.

## **1.5 Tujuan Penelitian**

Dalam melaksanakan penelitian ini tujuan yang ingin dicapai diantaranya adalah :

1. Untuk menganalisis bagaimana penerapan teknik *port knocking* dapat meningkatkan keamanan jaringan di PT. Rizano Cipta Mandiri dengan mencegah ancaman peretasan dan serangan dari luar yang dapat mengeksplorasi kerentanannya.
2. Untuk mengevaluasi bagaimana penerapan *port blocking* pada jaringan PT. Rizano Cipta Mandiri dapat mengurangi risiko insiden jaringan yang dapat mempengaruhi kinerja, produktivitas, dan reputasi perusahaan, serta untuk mengidentifikasi potensi ancaman yang dapat dihindari dengan pembatasan akses *port*.
3. Untuk menganalisis penerapan *firewall filtering* pada *MikroTik RouterOS* dalam mengatasi masalah keamanan jaringan di PT. Rizano Cipta Mandiri, serta menilai efektivitas penggunaan *firewall filtering* dalam memperkuat sistem keamanan jaringan perusahaan, dan mengevaluasi peran *MikroTik RouterOS* dalam menghadapi ancaman jaringan serta mengelola trafik data secara optimal.

## **1.6 Manfaat Penelitian**

Manfaat dari penelitian ini yaitu :

1. Dengan Penelitian ini diharapkan dapat memberikan solusi praktis dalam meningkatkan keamanan jaringan perusahaan, sehingga dapat melindungi data sensitif dan menjaga kontinuitas operasional. Dengan penerapan metode yang tepat, perusahaan dapat mengurangi risiko serangan siber yang dapat merugikan.
2. Penelitian ini dapat memberikan panduan praktis bagi administrator jaringan dan profesional TI dalam menerapkan sistem keamanan yang efektif menggunakan metode *Port Knocking*, *Port Blocking*, dan *Firewall Filtering*, sehingga meningkatkan ketahanan jaringan terhadap ancaman siber.

## **1.7 Gambaran Umum Objek Penelitian**

Dalam bagian ini diuraikan informasi objek penelitian sebagai gambaran umum yang berisikan sekilas tentang objek penelitian, visi & misi, dan struktur organisasi.

### **1.7.1 Sekilas Tentang PT. Rizano Cipta Mandiri**

Produk makanan dan minuman merupakan barang yang diperlukan pada kehidupan sehari-hari. Tingginya permintaan terhadap produk makanan dan minuman di zaman modern yang serba cepat ini memaksa perusahaan-perusahaan dalam bidang ini untuk bersaing dalam mempercepat dan meningkatkan efisiensi proses pemasaran, guna mendapatkan kepercayaan konsumen dan menghindari persaingan dari perusahaan sejenis. Dengan meningkatnya kebutuhan efisiensi

waktu, perusahaan harus memiliki koneksi jaringan yang memadai untuk memenuhi kebutuhan tersebut.

PT. Rizano Cipta Mandiri yang beralamat di Jl. By Pass Km 15 Aie Pacah, Padang, Sumatera Barat. Masrizal M. merupakan Direktur Utama saat ini memiliki karyawan pekerja 57 orang serta dilengkapi dengan kendaraan operasional 5 *mobil engkel*. Untuk nomor telepon yang dapat dihubungi 0752-574831. Dan jam operasional pada PT. Rizano Cipta Mandiri yaitu buka setiap hari senin sampai sabtu serta melayani pelanggan dari pukul 07.00 pagi hingga pukul 21.00 malam.

PT. Rizano Cipta Mandiri sudah dikenal di daerah Aie Pacah sebagai pemasok (distributor) makanan dan minuman yang mampu memenuhi kebutuhan produk masyarakat kota Padang. PT. Rizano Cipta Mandiri telah menjadi pilihan terbaik bagi masyarakat dalam membeli produk makanan dan minuman, karena menyediakan barang yang berkualitas, harga yang kompetitif, serta beragam jenis produk yang lengkap. Selain itu, sikap ramah dari tim sales juga menjadi faktor kunci mengapa perusahaan ini terus dipercaya oleh konsumen.

### **1.7.2 Visi & Misi PT. Rizano Cipta Mandiri**

Adapun Visi dan Misi yang ditetapkan dan diterapkan oleh PT. Rizano Cipta Mandiri yaitu :

#### **1. Visi**

Menjadi pelopor perusahaan sebagai pemasok produk terbaik dan terpercaya kepada konsumen dalam memenuhi kebutuhan produk makanan dan minuman. PT. Rizano Cipta Mandiri memiliki visi untuk “Menjadi

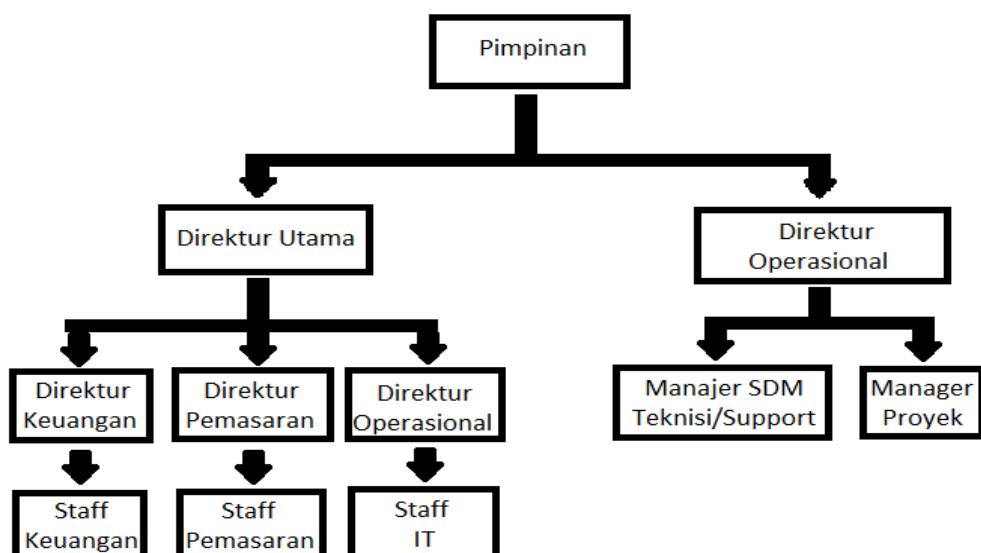
perusahaan terkemuka dalam bidang distribusi makanan dan minuman, diakui atas inovasi dan kualitas layanan yang ditawarkan.”.

## 2. Misi

- 1) Memberikan produk dan layanan terbaik kepada customer.
- 2) Menjadi pelopor ditribusi produk makanan dan minuman terkemuka.
- 3) Meningkatkan kepuasan customer.
- 4) Membangun hubungan jangka panjang yang saling menguntungkan.

### 1.7.3 Struktur Organisasi Toko

Dengan adanya struktur organisasi diharapkan akan dapat diketahui dengan jelas mengenai tugas, wewenang, dan tanggung jawab di PT. Rizano Cipta Mandiri. Adapun struktur organisasi PT. Rizano Cipta Mandiri dapat dilihat pada gambar 1.1 sebagai berikut :



Sumber : PT. Rizano Cipta Mandiri

**Gambar 1.1 Struktur Organisasi PT. Rizano Cipta Mandiri**

#### **1.7.4 Tugas dan Tanggung Jawab**

Berikut adalah uraian pekerjaan pada PT. Rizano Cipta Mandiri :

1. Pimpinan mempunyai tugas dan tanggung jawab sebagai berikut :
  - a. Menetapkan visi, misi, dan tujuan jangka panjang perusahaan.
  - b. Mengembangkan dan mengimplementasikan rencana strategis untuk mencapai tujuan tersebut.
2. Direktur Utama mempunyai tugas dan tanggung jawab sebagai berikut :
  - a. Bertanggung jawab atas keseluruhan operasional perusahaan.
  - b. Mengatur perencanaan strategis.
  - c. Pengaturan gaji karyawan.
  - d. Serta memiliki hak penuh atas pengambilan keputusan.
3. Direktur Keuangan mempunyai tugas dan tanggung jawab sebagai berikut :
  - a. Mengelola aspek keuangan perusahaan.
  - b. Pengelolaan akuntansi dan perencanaan keuangan.
4. Direktur Operasional mempunyai tugas dan tanggung jawab sebagai berikut:
  - a. Bertanggung jawab atas operasional sehari-hari.
  - b. Memanajemen proyek dan pengawasan proses produksi atau layanan.

5. Direktur Pemasaran mempunyai tugas dan tanggung jawab sebagai berikut:

- a. Mengelola strategi pemasaran,
- b. Mengelola penjualan, dan hubungan pelanggan untuk meningkatkan pangsa pasar.

6. Manajer Sumber Daya Manusia (SDM) mempunyai tugas dan tanggung jawab sebagai berikut :

- a. Bertanggung jawab atas pengelolaan SDM.
- b. Serta Pengelolaan rekrutmen, pelatihan, dan pengembangan karyawan.

7. Manajer IT mempunyai tugas dan tanggung jawab sebagai berikut :

- a. Mengelola infrastruktur teknologi informasi dan keamanan jaringan.
- b. Memanajemen pengembangan perangkat lunak dan dukungan teknis.