BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

PT DAK (PT Dok dan Perkapalan Air Kantung) merupakan sebuah perusahaan galangan kapal yang bergerak dalam bidang *Ship Repair, Ship Building, Docking* dan *Repair Engineering, Construction, Ship Equipment Supplies* dengan spesialisasi dalam pembuatan kapal dan perbaikan kapal yang memanfaatkan layanan jaringan internet dari *ISP* (*Internet Service Provider*) *Indihome* serta *mikrotik routerboard* sebagai pusat pengelolaan jaringannya untuk saling bertukar informasi data dan *file*. Semakin banyak jumlah komputer (*user*) yang terhubung di jaringan lokal maupun publik pada PT DAK (PT Dok dan Perkapalan Air Kantung) maka probabilitas ancaman dan serangan pada sistem keamanan jaringan tentu tidak dapat dihindari.

Keamanan jaringan merupakan sistem yang dipakai agar terhindar dari ancaman luar yang dapat merusak jaringan serta ancaman dari dalam, seperti ancaman pencurian data perusahaan, jebolnya sistem karena *password* yang diketahui oleh orang yang tidak berhak dan segala macam serangan dan usaha-usaha penyusupan atau pemindaian dengan cara memberikan proteksi atau perlindungan pada *router Mikrotik*. Proteksi dan keamanan pada *router Mikrotik* sangatlah penting untuk menjaga kelangsungan jaringan komputer perusahaan. Terutama untuk menjaga *router Mikrotik* dari segala macam akses *ilegal* yang mencoba untuk masuk dan mengelola jaringan pada *router mikrotik* perusahaan.

Permasalahan keamanan jaringan pada PT DAK (PT Dok dan Perkapalan Air Kantung) sering terjadi di karenakan terdapat *port-port* yang terbuka dan menyebabkan pengguna yang tidak valid dapat mengakses dan mengelola jaringan di *router mikrotik* perusahaan secara *ilegal*. Saat ini dalam sistem keamanan jaringan di PT DAK (PT Dok dan Perkapalan Air Kantung) belum terdapat sistem keamanan pada akses layanan *port* (*port service*) dalam mengatasi

serangan pada *winbox (8291), webfig (80),* dan *telnet (23).* Layanan *port* tersebut befungsi agar administrator jaringan dapat mengakses ke *router* dalam rangka melakukan pengelolaan jaringan di PT DAK (PT Dok dan Perkapalan Air Kantung). Salah satu cara untuk memproteksi *Mikrotik* dari serangan terhadap *port-port* yang terbuka dapat dihindari dengan menggunakan *Port Knocking* dan *Port Blocking.* Dengan melakukan *blocking* pada beberapa *port* yang rentan seperti *Telnet, Ssh,* ataupun *Winbox* dan hanya membuka akses tersebut hanya untuk administrator jaringan saja[3]. Dengan cara ini administrator jaringan dapat melakukan pengelolaan jaringan di *router mikrotik* secara lebih aman. *Port Knocking* dan *Port Blocking* bekerja dengan cara menutup semua *port* yang ada pada sistem komputer dan hanya administrator jaringan saja yang dapat mengakses sebuah *port* yang telah ditentukan yaitu dengan cara mengetuk atau *knock* terlebih dahulu[4]. Berdasarkan uraian tersebut maka di perlukan pemanfaatan metode *port knocking* dan *port blocking* dalam sistem keamanan jaringan.

Metode *Port Knocking* merupakan metode yang digunakan untuk membuka akses ke *port* tertentu yang telah ditolak oleh *firewall* pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa *protocol TCP, UDP* maupuan *ICMP*. Jika koneksi yang dikirimkan oleh *host* tersebut sudah sesuai dengan *rule knocking* yang diterapkan, maka secara dinamis *firewall* akan memberikan akses ke *port* yang sudah ditolak. *Firewall* merupakan sebuah sistem atau perangkat yang memberi otorisasi pada lalu lintas jaringan komputer yang dianggapnya aman untuk melaluinya dan melakukan pencegahan terhadap jaringan yang dianggap tidak aman [1]. *Firewall* berada diantara kedua jaringan seperti *internet* dan komputer. Didalam *router mikrotik* terdapat *fitur firewall* yang berfungsi untuk melindungi dengan cara memutus atau menerima sebuah paket yang akan masuk, melewati, atau keluar *router*. *Firewall* yang bisa diterapkan untuk melindungi serangan dari para *hacker* adalah *Port Knocking* dan *Port Blocking* [3].

Dari permasalahan tersebut, maka penulis berkeinginan untuk melakukan penelitian dengan judul **"**Implementasi Keamanan Jaingan Menggunakan Metode *Port Knocking* dan Port Blocking Pada *Router Mikrotik* Di PT DAK**".**

Adapun penelitian yang menjadi acuan dalam penulisan skripsi ini antara lain, penelitian yang dilakukan oleh Amarudin, pada tahun 2018 mengenai "Analisis Dan Implementasi Keamanan Jaringan Pada *Mikrotik Router OS* Menggunakan Metode *Port Knocking*"[1], Penelitian selanjutnya yaitu penelitian dari Randi Rizal, Ruuhwan, Kelvin Ajie Nugraha, pada tahun 2020 mengenai "Implementasi Keamanan Jaringan Menggunakan Metode *Port Blocking* dan *Port Knocking* Pada *Mikrotik RB-941*"[2], Selanjutnya penelitian oleh D. Demira, dan R. Wiryadinata pada tahun 2022 mengenai "Rancang Bangun Keamanan *Port Secur Shell (SSH)* Menggunakan Metode *Port Knocking*"[3], Penelitian selanjutnya yaitu penelitian oleh Januar Al Amin pada tahun 2020 mengenai "Implementasi Keamanan Jaringan Dengan *IP Table* Sebagai *Firewall* Menggunakan *Metode Port Knocking*"[4], Selanjutnya penelitian oleh M Julkarnain dan A Afahar pada tahun 2021 mengenai "Implementasi *Port Knocking* Untuk Keamanan Jaringan Smk 1 Sumbawa Besar"[5], Ahmad Zafrullah Mardiansyah, Yayank Muhammad Abdussyakur, Andy Hidayat Jatmika, pada tahun 2021 mengenai "Optimasi *Port Knocking* dan *Honeypot* Menggunakan *Ip Tables* Sebagai Keamanan Jaringan Pada Server"[6].

1.2 Rumusan Masalah

Berdasarkan dari latar belakang diatas, maka rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana metode *port knocking* dan *port blocking* bisa mengamankan akses ke *router mikrotik*?
2. Bagaimana mengimplementasikan *port knocking* dan *port blocking* pada keamanan *router mikrotik*?
3. Bagaimana menutup *port-port* yang terbuka pada *router mikrotik*?

1.3 Batasan Masalah

Adapun batasan masalah yang dibatasi agar dapat megacu pada implementasi keamanan jaringan menggunakan metode *port knocking* dan *port blocking* adalah sebagai berikut :

1. Penulis hanya mengimplementasikan *Port Knocking* dan *Port Blocking* pada *Mikrotik RouterBoard RB750Gr3*
2. Penulis hanya menggunakan 1 laptop untuk mengimplementasikannya
3. Penulis menggunakan koneksi internet dari Modem Telkomsel Flash
4. Dalam pengujian pengetukan *port*, penulis menggunakan *software PuTTY, Command Prompt*, dan *software Nmap*
5. Pengujian *port knocking* dan *port blocking* hanya menggunakan *Ping, Telnet*, dan *Ssh*
6. Penulis menggunakan *winbox v3.31*
7. Pengujian hanya menggunakan 1 *client*

1.4 Tujuan dan Manfaat Penelitian

Adapun tujuan dan manfaat penelitian adalah sebagai berikut :

1.4.1 Tujuan Penelitian

Adapun tujuan penelitian ini sebagai berikut :

1. Untuk meimplementasikan metode *port knocking* dan *port blocking* pada *router mikrotik*
2. Untuk meningkatkan keamanan pada *router mikrotik*
3. Untuk mengurangi terjadinya serangan pada *router mikrotik*
4. Untuk mencegah akses ilegal terhadap *router mikrotik*

1.4.2 Manfaat Penelitian

Adapun manfaat penelitian ini sebagai berikut :

1. Dapat mengoptimalkan keamanan jaringan komputer
2. Sebagai solusi untuk mengamankan *router mikrotik* dari hak akses yang *ilegal*
3. Dapat meningkatkan rasa aman bagi pengguna *router mikrotik*

1.5 Sistematika Penulisan

Sistematika penulisan skripsi ini dibuat agar lebih mudah dalam pembahasan, namun merupakan sau kesatuan antara bab yang satu dengan bab yang lainnya. Adapun susunan dari uraian bab-bab tersebut adalah :

BAB I : PENDAHULUAN

Bab ini berisikan mengenai latar belakang masalah, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, dan sistematika penulisan. Yang berfungsi sebagai penghantar bagi para pembaca untuk mengetahui hal apa saja yang akan dibahas secara keseluruhan.

BAB II : LANDASAN TEORI

Bab ini menerangkan tentang teori-teori yang digunakan untuk mendukung implementasi keamanan jaringan di PT DAK (PT Dok dan Perkapalan Air Kantung).. Dan mendasari pembahasan secara detail. Pada bab ini juga dituliskan tentang tools/software (komponen) yang digunakan untuk keperluan penelitian, tinjauan Pustaka, dan menguraikan teori-teori yang mendukung judul. Pada bab ini, uraian teori yang digunakan adalah uraian pendukung sesuai dengan topik yang diambil.

BAB III : METODOLOGI PENELITIAN

Bab ini berisi tentang metode penelitian yang digunakan dalam penelitian ini secara ringkas dan *komprehensif.*

BAB IV : HASIL DAN PEMBAHASAN

Dalam bab ini menjelaskan tentang riset, analisis masalah sistem yang berjalan, analisis hasil solusi, analisis kebutuhan sistem ususlan , analisis sistem, dan perancangan sistem, serta implementasi dan pengujian sistem..

BAB V : PENUTUP

Pada bab ini berisi kesimpulan dan saran dari laporan yang telah dibuat agar ada pengembangan yang lebih baik untuk masa yang akan datang.