BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan sistem informasi adalah suatu langkah pencegahan terhadap tindakan penipuan pada sistem yang berbasis informasi berbentuk non-fisik dan dilakukan untuk memastikan bahwa data dalam suatu sistem terlindungi dari ancaman. Tidak hanya ancaman penipuan, bentuk ancaman dari serangan siber lainnya pun harus dicegah. Ancaman tersebut bisa berupa serangan dari luar seperti *hacking*, *virus*, atau *malware*, maupun dari dalam seperti kebocoran data oleh oknum karyawan.

Jaringan komputer merupakan media penghubung untuk pertukaran data dan informasi. Oleh karena itu dibutuhkan keamanan Jaringan untuk menjaga dan menjamin keamanan data. Dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak bertanggung jawab.

Keamanan jaringan merupakan aspek terpenting sebuah sistem dalam menjaga validitas dan integritas data, serta menjamin ketersediaan layanan bagi penggunaannya. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak (A. Z. Mardiansyah *et al*., 2021).

Sistem jaringan komputer dirancang dengan tujuan dapat berbagi sumber daya untuk dipakai secara bersama. Pada proses berbagi sumber daya, keamanan dan kerahasiaan data menjadi isu utama, sehingga apabila terjadi serangan *cyber* akan menyebabkan kerugian. Hal penting yang perlu diperhatikan adalah *Confidentiality*, *Integrity* and *Availability* (CIA) yang merupakan standar untuk mengevaluasi dan menerapkan keamanan informasi (T. Ernawati *et al*., 2021).

Kebutuhan akan jaringan komputer semakin bertambah penting, baik dalam pendidikan, pekerjaan maupun dalam sebuah permainan, dengan banyaknya akses ke

jaringan tersebut maka akan banyak pula peluang kejahatan yang terjadi didalam jaringan ataupun adanya peretas yang dapat mematikan sumber daya pada *server*.

Pada penelitian ini peneliti menerapkan konfigurasi melalui *firewall*, dengan menerapkan *Port Knocking*. *Port Knocking* adalah teknik keamanan yang digunakan untuk mengamankan akses ke sistem atau layanan jaringan dengan cara memungkinkan akses ke *port-port* tertentu hanya setelah urutan tertentu dari koneksi ke *port-port* lain telah terjadi. Dalam istilah yang lebih sederhana, *Port Knocking* memungkinkan pengguna atau server untuk membuka akses ke *port* tertentu dengan mengirimkan serangkaian permintaan koneksi ke *port-port* lain sebelumnya. Keuntungan dari teknik *Port Knocking* adalah mempersulit serangan *brute-force* atau serangan lainnya yang mencoba memindai *port-port* yang aktif dan menemukan celah keamanan. Penting untuk diingat bahwa meskipun teknik ini dapat menambahkan lapisan keamanan tambahan, itu tidak sepenuhnya aman jika diimplementasikan tanpa tindakan keamanan lainnya. *Port Knocking* seringkali digunakan bersama dengan teknik keamanan lainnya untuk menciptakan sistem yang lebih aman.

Konfigurasi selanjutnya yang dilakukan yaitu *Honeypot*. *Honeypot* adalah sebuah sistem atau perangkat lunak yang didesain dengan sengaja untuk menarik perhatian penyerang atau pihak yang mencoba mengeksploitasi kelemahan keamanan dalam suatu jaringan komputer atau sistem. *Honeypot* berfungsi sebagai umpan atau perangkap yang bertujuan untuk menarik serangan sehingga peneliti keamanan atau administrator jaringan dapat mempelajari metode serangan tersebut, mengidentifikasi ancaman baru, dan memahami taktik penyerang. *Honeypot* digunakan sebagai alat pembelajaran dan pemahaman terhadap ancaman siber. Implementasi *Honeypot* harus dilakukan dengan hati-hati dan diisolasi dengan baik agar tidak membahayakan keamanan sistem dan jaringan yang sebenarnya.

Konfigurasi selanjutnya yang dilakukan yaitu *IPTables*. *IPTables* adalah perangkat lunak *firewall* yang digunakan pada sistem operasi Linux untuk mengelola aturan-aturan keamanan jaringan. Dengan menggunakan *IPTables*, pengguna dapat mengkonfigurasi aturan-aturan untuk mengontrol lalu lintas jaringan yang masuk dan keluar dari sistem, serta memungkinkan atau memblokir koneksi ke atau dari *port-port* tertentu. *IPTables* digunakan untuk mengamankan sistem Linux dari serangan jaringan, mengontrol akses ke layanan jaringan, dan melindungi sistem dari ancaman siber. *IPTables* bekerja dengan memeriksa paket-paket data yang melewati sistem dan membandingkannya dengan aturan-aturan yang telah ditetapkan.

Pada penelitian Dian Novianto, *et al*. (2023) meneliti tentang peningkatan keamanan mikrotik, menggunakan *Port Knocking* dan *Port Blocking*. Data yang digunakan yaitu hasil dari konfigurasi yang telah dilakukan. Hasil pengujian ini dapat mengamankan akses ke router mikrotik dengan cara terlebih dahulu mengirimkan paket *knocking* berupa ping ke *IP Address*, *Telnet*, dan *SSH*.

Pada penelitian selanjutnya oleh Agus Riki Gunawan, *et al*. (2021) meneliti tentang pendeteksi dan pencegah *malware*, menggunakan *S*ystem *Snort* dan *Honeypot.* Data yang digunakan diambil dari port scanning oleh *S*ystem *Snort* dan *Honeypot* terkumpul selama 1 bulan mulai bulan Februari 2020 – Maret 2020 menggunakan *Snort IDS* dan *Honeypot*. Hasil dalam penelitian ini mengungkapkan dapat mencegah 248.574 data serangan dengan 11 atribut, yang setiap atributnya dapat mendeteksi IP penyerang dan tanggal penyerangan.

Pada penelitian selanjutnya oleh Nur Rohman Rosyid, *et al*. (2022) meneliti tentang deteksi malware pada jaringan lokal, menggunakan *Honeypot* dan *Yara*. Data yang digunakan diambil dari pengujian sistem dilakukan menggunakan 2 sensor *Honeypot* yang dipasang pada jaringan public dan server proaktif menggunakan 409 *Yara rules malware*. Hasil dari penelitian ini yaitu dalam mendeteksi *malware* telah berhasil dilakukan dan memiliki potensi sebagai mekanisme keamanan proaktif yang membantu meningkatkan kualitas mitigasi resiko keamanan siber di era industri 4.0.

Pada penelitian selanjutnya oleh Randi Rizal, et al. (2020) meneliti tentang implementasi keamanan jaringan, menggunakan metode *Port Blocking* dan *Port Knocking* pada Mikrotik RB-941. Data yang digunakan diambil dari tiga tahap utama yang dilakukan yaitu analisis data port yang akan di uji. Hasil dalam pengimplementasian *Port Blocking* dan *Port Knocking* dalam pengamanan jaringan lokal mengungkapkan bahwa *Port Blocking* dan *Port Knocking* memiliki kelebihan dan kekurangannya masing-masing.

Pada penelitian selanjutnya oleh Ahmad Zafrullah Mardiansyah, *et al*. (2021) meneliti tentang optimasi keamanan jaringan pada server, menggunakan metode *Port Knocking*, *Honeypot* dan *IPTables*. Data yang digunakan diambil dari berbagai konfigurasi yang dilakukan dan telah dilakukan pengujian. Hasil dari penelitian ini adalah penambahan metode *IPTables* dapat meningkatkan kinerja baik dari segi penggunaan CPU (38,4%) dan Memori (44,2%) pada server maupun keamanan jaringan dibandingkan dengan hanya menggunakan metode *Port Knocking* dan *Honeypot* saja.

Berdasarkan uraian latar belakang diatas, maka akan dikaji lebih dalam permasalahan ini dengan mengangkat judul "**ANALISIS PERBANDINGAN TINGKAT OPTIMALISASI PORT KNOCKING DAN HONEYPOT MENGGUNAKAN IPTABLES PADA SERVER UNTUK KEAMANAN JARINGAN**".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, agar permasalahan tidak terlalu melebar sehubungan dengan keterbatasan waktu, anggaran, dan kemampuan melaksanakan penelitian, maka dirumuskan permasalahan seperti berikut:

1. Bagaimana meningkatkan keamanan *Port Knocking* dan *Honeypot* menggunakan metode *IPTables* untuk keamanan jaringan pada server dengan sumber daya yang lebih rendah dan lebih tinggi?
2. Bagaimana meningkatkan Kinerja *Port Knocking* dan *Honeypot* menggunakan metode *IPTables* untuk keamanan jaringan pada server dengan sumber daya yang lebih rendah dan lebih tinggi?
3. Apakah penambahan *IPTables* dalam keamanan jaringan dapat mengatasi serangan *Denial of Service* (*DoS*) dan *Brute Force*?

1.3 Batasan Masalah

Berdasarkan uraian diatas agar dalam penyusunan penelitian tesis ini menjadi lebih terarah dan tidak menyimpang dari tujuan pembahasan, maka penulis membatasi pokok permasalahan yang akan dibahas pada penelitian sebagai berikut:

1. Penelitian dilakukan untuk membandingkan keamanan jaringan *Port Knocking* dan *Honeypot* menggunakan metode *IPTables* pada server dengan sumber daya yang lebih rendah dan lebih tinggi.
2. Penelitian dilakukan dilakukan untuk menguji *Port* mana saja yang terserang dan bagaimana dampaknya terhadap sumber daya CPU dan Memori server.
3. Penyerangan dilakukan dengan menggunakan *Denial of Service* (*DoS*) dan *Brute Force*.

1.4 Tujuan Penelitian

Berdasarkan uraian sebelumnya agar dalam penyusunan penelitian tesis ini menjadi lebih terarah dan memiliki tujuan yang jelas, maka penulis menentukan tujuan dalam penelitian ini sebagai berikut:

1. Meningkatkan keamanan *Port Knocking* dan *Honeypot* menggunakan metode *IPTables* untuk keamanan jaringan pada server dengan sumber daya yang lebih rendah dan lebih tinggi.
2. Meningkatkan Kinerja *Port Knocking* dan *Honeypot* menggunakan metode *IPTables* untuk keamanan jaringan pada server dengan sumber daya yang lebih rendah dan lebih tinggi.
3. Membuat penambahan *IPTables* dalam keamanan jaringan dapat mengatasi serangan *Denial of Service* (*DoS*) dan *Brute force*.

1.5 Manfaat Penelitian

Melalui penelitian tesis ini penulis berharap dapat memberikan sumbangan pemikiran dan manfaat baik bagi peneliti, perusahaan dan peneliti selanjutnya, sehingga peneliti mengharapkan manfaat sebagai berikut:

1. Dapat mengetahui manfaat keamanan jaringan menggunakan metode *Port Knocking* dan *Honeypot* menggunakan *IPTables* sebagai keamanan jaringan pada *server*.
2. Dapat menjadi referensi bagi pengembang keamanan jaringan untuk menentukan metode yang akan digunakan sesuai dengan kebutuhannya.
3. Dapat menjadi referensi untuk penelitian yang akan dilakukan selanjutnya.

1.6 Sistematika Penulisan

Sistematika penulisan tesis ini dibuat agar dapat menjadi pedoman atau garis besar penulisan sehingga memudahkan pembacaan dan pemahaman, laporan penulisan ini dan dapat menggambarkan secara jelas isi dari laporan penelitian, oleh karena itu penulis dalam menyusun tesis memuat beberapa bab tergantung bagaimana permasalahan yang disajikan. Sistem penulisan laporan penelitian ini terdiri dari:

BAB I PENDAHULUAN

Bab ini penulis memberikan gambaran mengenai latar belakang permasalahan, rumusan masalah, batasan, tujuan, manfaat dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas beberapa tinjauan Pustaka berupa hasil penelitian sebelumnya yang dijadikan acuan dalam penulisan tesis ini. Dijelaskan juga teori-teori yang berkaitan dengan penelitian tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Bab ini berisikan langkah-langkah penelitian yang akan dilakukan, rancangan keamanan yang akan digunakan, dan skenario pengujian.

BAB IV ANALISIS DAN PERANCANGAN

Bab ini membahas tentang analisis keamanan jaringan komputer dan perancangan untuk melakukan penelitian meningkatkan keamanan jaringan menggunakan *Port Knocking*, *Honeypot* dan *IPTables*.

BAB V PENGUJIAN DAN PERBANDINGAN HASIL

Bab ini berisikan hasil pengujian menggunakan *Denial of Service* (DoS) dan *Brute Force* setelah penambahan *IPTables*, serta melakukan perbandingan dari hasil penyerangan sebelum dan sesudah menggunakan *IPTables.*

BAB VI PENUTUP

Bab ini berisi kesimpulan–kesimpulan yang didapat dari hasil penelitian dan saran-saran untuk perbaikan/mengevaluasi terhadap apa yang telah dijelaskan sebelumnya.