

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Perkembangan Teknologi jaringan terutama sistem keamanan jaringan yang semakin berkembang menuntut agar sistem keamanan untuk berkembang, terutama pada keamanan *server* yang merupakan salah satu tugas pokok dari sistem jaringan. Hal ini didasarkan pada karakteristik umum dari jaringan komputer yang pada dasarnya adalah tidak aman untuk diakses secara bebas. Terbukanya *port* untuk layanan yang bersifat *public* maupun bersifat privat, memiliki kemungkinan resiko yang tinggi untuk diserang oleh para *attacker*.

Jaringan adalah sebuah sistem operasi yang terdiri atas beberapa jumlah komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama atau suatu jaringan kerja yang terdiri dari titik-titik yang terhubung satu sama lain, atau bisa diartikan komunikasi antar perangkat. Banyaknya perangkat yang saling terhubung dalam sebuah jaringan komputer akan menimbulkan akses yang tidak diinginkan antara perangkat. Untuk meminimalisir atau menghindari masalah tersebut dibutuhkan sistem keamanan jaringan.

Sistem Keamanan Jaringan adalah proses untuk mencegah dan mengidentifikasi pengguna yang tidak sah (*peyusup*) dari jaringan komputer. Tujuannya adalah untuk mengantisipasi resiko jaringan komputer yang dapat berupa ancaman fisik maupun *logic*. dimaksud fisik itu adalah yang merusak bagian fisik komputer sedangkan ancaman *logic* yaitu pencurian data atau penyusupan akun seseorang. Orang yang tidak bertanggung jawab dapat menggunakan program untuk melakukan penyerangan terhadap jaringan. Banyak

teknik penyerangan terhadap jaringan yang dapat diterapkan, salah satunya melalui *port*. *Port* adalah sokcet atau jack koneksi yang berada diluar unit sistem.

*Port knocking* adalah bentuk komunikasi antara dua komputer, di mana informasi di salurkan melalui *port-port* yang tertutup. Di mana informasi yang di kirimkan harus melalui proses *encode* ke dalam bentuk usaha untuk membangun koneksi ke *port* dengan urutan tertentu. Usaha untuk membangun koneksi ke *port* bisa disebut juga ketukan (*knock*), yakni dimana *port knocking* ini akan memberikan keamanan lebih kepada *server* karena sistem pengetukan *port* yang dilakukan secara sehingga *port* yang diketuk untuk membuka *port* utama tidak akan mudah untuk termonitoring. Dengan buat beberapa *port* yang akan diketuk, metode *port knocking* ini maka setiap *port* yang diketuk pada setiap sesinya akan berbeda-beda sehingga integritas keamanan dapat lebih di tingkatkan.

Dalam penelitian sebelumnya tentang Penerapan Sistem Keamanan Jaringan Menggunakan *Random Port Knocking* Berbasis *Raspberry Pi* yang dikirm melewati *Telegram* dilakukan oleh Iga Revva Princiss, Jeinever, Abdul Rasyid, dan Nugroho Suharto menunjukkan bahwa untuk metode yang diterapkan membuat *server* aman. Karena pengacakan *port* dan *block* IP membuat pihak yang tidak bertanggung jawab akan berusaha lebih keras untuk menembus dinding *firewall*.

Berdasarkan penilitian diatas, penulis ingin mencoba mengimplementasikan keamanan *server* menggunakan metode *port knocking* dengan mengirimkan pesan serangan ke *telegram* sebagai notifikasi untuk *sysadmin* mengetahui adanya serangan yang dilakukan seorang *attacker* yang mencoba *login* ke dalam *server* melalui *port* ssh sehingga di harapkan sistem yang di bangun menangani keamanan jaringan dan masalah pencurian data dan informasi, dengan memanfaatkan *port knocking* dan *honeypot* (*server* bayangan)

untuk meningkatkan keamanan jaringan komputer pada *server* dari *attacker*.

Dari pembahasan latar belakang diatas penulis melakukan penelitian dengan judul “Implementasi Keamanan *Remote Server* Memggunakan Metode *Port Knocking* Dengan Mengirimkan Ke *Telegram* Sebagai Notifikasi”.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah di paparkan, didapatkan masalah yang perlu diselesaikan dan menjadi dasar dalam pengerjaan penelitian ini yaitu bagaimana cara mengamankan *server* dari serangan *attacker* dengan menggunakan metode *port knocking* yang nantinya *notifikasi* dikirim ke akun *social media telegram* pada administrator jaringan.

## 1.3 Batasan Masalah

Untuk memperarah tujuan dari penelitian ini, penulis membuat beberapa batasan masalah yaitu:

1. *Port* yang diteliti adalah *port SSH (port 22)*.
2. Penelitian ini difokuskan bagaimana cara kerja metode *port knocking* dalam meremote *server* dan mengamankannya dari serangan para *attacker*.
3. *Aplikasi social media* yang di gunakan adalah *telegram*.

## 1.4 Tujuan Penelitian

Dari permasalahan-permasalahan yang didapat, tujuan yang ingin dicapai pada penelitian ini yaitu dapat menerapkan metode *port knocking* untuk menamankan *port ssh* dalam meremote *server*.

## 1.5 Manfaat Penelitian

Adapun beberapa manfaat dari penelitian ini ialah:

1. Penelitian ini di harapkan dapat lebih mendalami lagi ilmu mengenai *server* untuk

mengamankannya.

2. Penelitian ini dapat diharapkan menambah wawasan mengenai metode *port knocking* dan *server* dalam mengamankannya.
3. Membantu untuk mengamankan *server* dari serangan dan pencurian data.

## **1.6 Sistematika Penulisan**

Sistematika dalam penulisan laporan skripsi ini terdiri dari berapa bab yang dapat dilihat sebagai berikut:

### **BAB I PENDAHULUAN**

Bab ini berisi latar belakang, perumusan masalah, batasan penelitian, tujuan penelitian, manfaat penelitian, serta sistematika penulisan.

### **BAB II TINJAUAN PUSTAKA**

Bab ini berisi teori yang menjadi acuan untuk pembuatan skripsi, dan juga membahas tentang penelitian-penelitian oleh pihak lain yang sejenis atau yang sama dengan topik ini.

### **BAB III METODE PENELITIAN**

Bab ini berisi metode penelitian yang digunakan, yang meliputi teknik pengumpulan data, alat dan bahan penelitian, jenis metode penelitian, analisis sistem yang berjalan, dan gambaran sistem yang akan dibuat.

### **BAB IV HASIL DAN PEMBAHASAN**

Pada bab ini menjelaskan implementasi perancangan detail dalam hal kerja sistem beserta analisis terhadap sistem serta pengujian.

### **BAB V PENUTUP**

Pada bab ini berisi kesimpulan yang didapatkan dari analisis mengenai keterkaitan dengan *user* dan sistem serta saran demi pengembangan sistem dimasa yang akan datang.