BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi pada zaman sekarang ini sangat berperan penting dalam kehidupan kita saat ini, salah satunya adalah pertukaran data yang sering dilakukan oleh banyak orang melalui jaringan internet. Untuk membantu pertukaran data itu bisa menggunakan FTP (file transfer protocol), dan FTP bisa digunakan untuk melakukan transfer data yang besar melalui jaringan internet. Karena media seperti email memiliki keterbatasan untuk mengirim ukuran file yang besar. FTP merupakan salah satu protokol internet yang paling awal di kembangkan, dan masih digunakan sampai saat ini untuk melakukan transfer data, download dan upload data komputer antara client FTP dan server FTP. FTP menggunakan metode autentikasi dengan username dan password untuk menambah privasi pada data yang akan di transfer. Namun dalam menjalankan fungsinya username dan password dikirim dalam bentuk tidak terenkripsi, transfer FTP terletak pada port 21 yang menggunakan port TCP (transmission control protocol) sebagai alat komunikasi data komputer pada client dan server. Port TCP nomor 21 digunakan sebagai port pengatur. Selain mempunyai port 21 FTP juga mempunyai port 20, yang akan terbuka sebagai koneksi transfer data. Dalam keadaan normal port untuk layanan FTP nomor 21 selalu terbuka walaupun sistemnya tidak digunakan untuk proses transfer data.

Banyaknya *hacker* dan *cracker* yang mencoba masuk kedalam FTP server untuk mengambil *file* penting, dengan adanya sistem *port knocking* dan fail2ban diharapkan untuk mencegah dan membuat FTP *server* menjadi aman dan mencegah serangan *brute force*. Serangan *brute force* merupakan serangan yang menyerang sistem keamanan jaringan pada saat melakukan *transfer file* pada FTP *server*. Serangan *brute force* adalah serangan secara paksa untuk *login* secara berulang dengan melakukan kesalahan *password*. Untuk mencegah serangan *brute force* terhadap keamanan jaringan di skripsi ini dapat mengimplementasikan fail2ban. Fail2ban bekerja dengan cara merubah aturan konfigurasi *firewall* dengan konfigurasi yang berada di fail2ban itu sendiri, ketika fail2ban berjalan, fail2ban akan mengambil alih fungsi *firewall* yang berada di *server.*

Pada peneltian sebelumnya *firewall* digunakan untuk menutup seluruh *port* dengan memberikan hak akses *client* yang dapat mengakses *server*, penggunaan *port knocking* mengharuskan *client* melakukan otentifikasi sebelum menggunakan layanan FTP. Hasil dari pengujian, dengan mengaktifkan *firewall* membuat peretas tidak dapat mengetahui *port* berapa yang aktif. Menggunakan sistem otenfitikasi *port knocking* dapat melindungi hak akses penggunaan layanan FTP.

Pada skripsi ini akan memberikan solusi bagaimana mencegah serangan *brute force* dengan menggunakan sistem *firewall*, *port knocking* dan fail2ban. *Firewall* akan memberikan keamanan untuk *memfilter* paket data dari luar maupun dalam *server*. *Port knocking* akan membuka dan menutup akses ke *port* yang telah di *block*, sehingga keamanan data *transfer file* akan sulit untuk di masukin oleh pengguna asing. Fail2ban akan bekerja untuk membatasi akses dan membuat aturan akses di *server*.

Pada skripsi ini *client* memiliki kenyamanan dan keamanan dalam melakukan *transfer file* pada FTP *server*. Keamanan dalam melakukan *transfer file* menjadi hal yang mutlak dalam sistem kemanan jaringan komputer, sehingga hal-hal yang tidak terduga tidak terjadi tehadap *server* seperti serangan *brute force* yang bisa dicegah dengan adanya *port knocking*, *firewall*, dan fail2ban dan dijalankan di dalam sistem operasi centos 7. Centos 7 merupakan sebuah *platform* komputasi berbasis linux yang mempunyai kelebihan yaitu mudah di modifikasi, aman dan stabil. Centos 7 juga memliki tingkat keamanan yang secara terus meneurs di perbarui, sehingga keuntungan dari skripsi ini sebagai keamanan data memiliki keuntungan yang lebih dan bermanfaat.

Berdasarkan uraian tersebut maka penulis tertarik untuk membuat sistem keamanan jaringan tentang "**IMPLEMENTASI PORT KNOCKING, FIREWALL, DAN FAIL2BAN SEBAGAI KEAMANAN DATA PADA FTP SERVER BERBASISKAN CENTOS7"**

1.2. Rumusan Masalah

Adapun rumusan permasalahan yang akan diselesaikan dalam penelitian ini adalah:

1. Bagaimana merealisasikan *port knocking*, *firewall*, dan fail2ban pada linux centos 7 untuk keamanan data transfer ?
2. Bagaimana melakukan pengujian *port knocking*, *firewall*, dan fail2ban pada FTP *server*?

1.3. Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut :

1. Mengimplementasikan *port knocking*, *firewall*, fail2ban pada linux centos 7 untuk kemanan data transfer
2. Menguji *port knocking*, *firewall* dan fail2ban pada FTP *server* pengujian dilakukan dengan menggunakan filezilla, *command promt dan* putty

1.4 Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. *Firewall* pada FTP *server* membuat penyerang tidak dapat mengetahui *port* mana saja yang sedang terbuka.
2. Mencegah serangan *brute force* pada FTP *server.*
3. Memberikan keamanan dan kenyamanan dalam melakukan transfer data pada *client.*

1.5 Batasan Masalah

Dengan rumusan masalah tersebut, maka diperlukan batasan masalah sehingga pembahasan dapat terarah sesuai dengan tujuan penelitian. Adapun batasan masalah tersebut adalah sebagai berikut :

1. Sistem operasi yang digunakan linux centos 7.
2. Hanya menggunakan 1 *server* dan 1 *client*.
3. Menggunakan *port knocking*, *firewall,* dan fail2ban pada FTP *server*.