BAB 1.PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi di era modern saat ini semakin berkembang dan berperan penting dalam kehidupan. Teknologi informasi yang membantu manusia untuk mempermudah menemukan informasi. Salah satu contohnya memberikan informasi melalui website. Dalam penggunaan website ada sebuah server yang berfungsi untuk menampung data-data yang disebut web server. Web server bertugas untuk menerima permintaan HTTP atau HTTPS yang dikirim oleh klien melalui web browser dan mengirimkan kembali hasilnya dalam bentuk HTML. Web server berguna sebagai tempat aplikasi web dan sebagai penerima request dari client (Indra Warman & Zahni, 2013).

Perkembangan teknologi yang semakin canggih dan modern menyebabkan semakin banyak jenis penyusupan ataupun serangan seperti pencurian data yang terjadi di jaringan tersebut ataupun adanya peretas website, itu semua disebabkan oleh suatu sistem keamanan yang kurang canggih atau tidak mumpuni. Jika serangan tidak terdeteksi maka akan menyebabkan kerugian pada jaringan yang digunakan.

Menurut Herman (2018) keamanan jaringan merupakan perlindungan dari sumber daya terhadap upaya perubahan dan perusakan oleh seseorang yang tidak diizinkan. Sifat jaringan komputer yang global dan pada dasarnya sangat tidak aman karena pada saat terjadinya pengiriman data dari suatu komputer ke komputer yang lain di dalam internet maka akan ada kesempatan bagi user untuk menyadap atau mengubah data yang melewati komputer yang terhubung didalam jaringan yang sama kecuali komputer yang terkunci di dalam ruangan dan mempunyai akses terbatas untuk tidak terhubung ke jaringan luar maka komputer tersebut aman. Pembobolan sistem keamanan sering terjadi dan hampir setiap hari terdeteksi adanya pembobolan sistem.

Setiap jaringan pasti ada celah untuk diretas oleh setiap pengguna yang tidak bertanggungjawab dan berusaha untuk masuk pada jaringan. Keamanan jaringan harus mempunyai integritas data yang tinggi. Serangan terhadap server bisa terjadi

setiap waktu. Sebelum mengamankan jaringan harus menganalisa resiko atau ancaman yang akan terjadi. Untuk itu jaringan komputer harus dianalisa agar tahu apa yang perlu diamankan. Untuk metode yang dipilih untuk tugas akhir ini adalah reverse proxy. Reverse proxy berfungsi untuk menutupi web server atau bisa dikatakan sebagai perantara antara server dan klien. Dengan metode reverse proxy maka web server akan aman selama port asli web server tidak diketahui.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, permasalahan diatas dalam tugas akhir ini adalah :

1. Mengapa memilih metode reverse proxy sebagai keamanan web server?
2. Mengapa menggunakan nginx sebagai reverse proxy?

1.3 Batasan Masalah

Berdasarkan latar belakang diatas maka disimpulkan untuk membuat batasan masalah sebagai berikut :

1. Website yang digunakan adalah tampilan default page debian.
2. Keamanan yang digunakan hanya Nginx dan menggunakan metode Reverse Proxy.
3. Untuk tugas akhir ini hanya bisa digunakan di jaringan private saja.
4. Tidak sampai menanggulangi serangan.

1.4 Tujuan

Berdasarkan rumusan masalah diatas, tujuan yang dapat diambil dalam tugas akhir ini adalah :

1. Menggunakan metode reverse proxy agar keamanan web server terjaga.
2. Nginx lebih mudah dikonfigurasi serta lebih ringan saat digunakan.

1.5 Manfaat

Tugas akhir yang berjudul Implementasi Keamanan Jaringan Web Server Menggunakan Nginx Dengan Metode Reverse Proxy dengan dibangunnya server ini diharapkan dapat mengatasi masalah serangan yang terjadi pada web server dan mencegah hal yang mengganggu lalu lintas data pada web server.