BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Pada era perkembangan teknologi yang sangat pesat pada teknologi saat ini salah satunya adalah komputer. Masyarakat sekarang banyak bergantung kepada teknologi, karena teknologi memudahkan seseorang untuk melakukan pekerjaannya denga cepat dan mudah. Mulai dari hiburan, transaksi online, promosi dan pekerjaan. Dalam dunia kerja misalnya banyak orang yang menggunakan komputer untuk mengirim data, data – data tersebut ada yang bersifat biasa dan bersifat penting *(private)*. Selain itu perkembangan internet yang cukup pesat membawa pengaruh yang cukup besar bagi pihak-pihak yang memanfaatkan internet ini. Seiring dengan kemajuan tersebut kebutuhan akan keamanan dan kelancaran dalam berinternet sangat diperlukan karena kemajuan teknologi internet berbanding lurus dengan kejahatan-kejahatan yang ada dalam internet itu sendiri. Dengan adanya kejahatan-kejahatan internet ini para pengguna semakin tidak aman dan menjadi intaian para penjahat setiap kali mereka berinternet, maka diperlukan solusi yang bisa membantu agar data yang dipertukarkan bisa aman dan bisa sampai ke tujuan sesuai dengan yang diinginkan. Salah satu solusi yang ditawarkan adalah dengan menggunakan metode enkripsi yaitu suatu metode yang digunakan untuk mengamankan data dengan mengubah data asli kedalam bentuk *unicode* dengan aturan tertentu. Ada beberapa metode enkripsi yang bisa digunakan diantaranya adalah dengan metode *Secure Shell*.

File Transfer Protocol (FTP) merupakan salah satu sarana untuk melakukan *sharing* data, dimana data tersebut tersimpan pada *directory* sebuah komputer *server* sehingga dapat diakses oleh sejumlah besar komputer secara bersamaan. FTP menggunakan autentikasi dengan *username* dan *password* untuk menambah privasi pada data yang di-*sharing* (Batara Sakti, Abdul Aziz, Afrizal Doewes, 2013).

Secure Shell (SSH) sebagai salah satu protokol keamanan jaringan, sering digunakan untuk mengamankan tranmisi FTP dengan memanfaatkan fungsi enkripsi pada SSH. Namun dengan semakin berkembangnya teknik-teknik serangan pada keamanan jaringan komputer, perlu dilakukan pengujian untuk mengukur tingkat keamanan SSH dalam mengamankan transmisi FTP (Batara Sakti, Abdul Aziz, Afrizal Doewes,2013).

Terutama banyak digunakan pada sistem *berbasis linux* (UNIX *like*) dan Unix untuk mengakses akun shell. SSH dirancang sebagai pengganti Telnet dan shell remote tak aman lainnya, yang mengirim informasi, terutama kata sandi, dalam bentuk *plain text* yang membuatnya mudan untuk disadap. Enkripsi yang digunakan oleh SSH menyediakan kerahasiaan dan integritas data melalui jaringan yang tidak aman seperti internet. SSH dapat digunakan untuk mentransfer file melalui SFTP atau SCP. SSH menggunakan client-server model. Standart TCP port 22 telah ditetapkan sebagai jalur untuk server FTP SSH dan port 21 telah ditetapkan sebagai jalur untuk server FTP biasa.

Enkripsi merupakan proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Sniffing bertujuan untuk membuktikan teori tentang kelemahan FTP

pada tranmisi data yang tidak terenkripsi dengan melihat perbandingan dari hasil yang didapat (Batara Sakti, Abdul Aziz, Afrizal Doewes,2013).

Pada penelitian sebelumnya berfokus pada cara menerapkan *penetration testing* pada sistem sesuai dengan kaidahnya dan cara mengukur tingkat keamanan implementasi SSH berdasarkan hasil *penetration testing* yang telah dilakukan. Pengujian dilakukan pada sistem yang dibangun sebagai objek penelitian dimana sistem tersebut terisolasi sehingga tidak memerlukan manajemen *user* secara mendetail dan penguji tidak memiliki *client*. Metode yang digunakan adalah *white-box testing* dimana pengujian dilakukan dari dalam jaringan dengan tanpa melalukan pengumpulan informasi terlebih dahulu karena informasi tentang sistem sudah diketahui secara lengkap. Pengujian ini berfokus pada *service* FTP dan SSH dimana sudah terdapat model ancaman berdasarkan teori dari kelemahan masing-masing *service*. Data-data tersebut akan berguna sebagai parameter untuk menentukan solusi keamanan pada sistem jaringan komputer lain yang serupa. Pada penelitian ini menggunakan beberapa implementasi penetration testing seperti vulnerability scanning, sniffing, brute force attack dan creating backdoor. Jadi penelitian membuktikan bahwa implementasi SSH secara standart tidak cukup efektif dalam mengamankan transmisi FTP. SSH secara standart terbukti hanya dapat melindungi transmisi FTP dari penyadapan pada fase *sniffing*. Teori tentang kelemahan SSH pada brute force root login terbukti benar dengan hasil yang didapat pada fase brute force dengan Hydra (Batara Sakti, Abdul Aziz, Afrizal Doewes, 2013). Tetapi jika anda menggunakan telnet, rlogin, dan ftp tanpa disadari bahwa password yang terkirim tanpa melalui enkripsi. Sedangkan

dengan menggunakan OpenSSH melakukan enkripsi kepada semua trafik (termasuk password), secara efektif untuk menghindari hal-hal yang tidak diinginkan. Open SSH memiliki tunneling yang aman dan beberapa metode autentikasi dan juga mendukung semua versi protokol SSH. Open SSH sangat tepat untuk bisa menggantikan rlogin dan telnet dengan program SSH dan FTP dengan SFTP (Ika Dwi Cahyani,2014).

Dari hasil-hasil penelitian sebelumnya, maka dapat disimpulkan bahwa suatu jaringan memerlukan cara pertukaran data-data dengan aman dan memiliki pelindung untuk menunjang tingkat keamanan. Pada jurnal acuan pertama menjelaskan pengamanan FTP server dengan Penetration Testing , sedangkan jurnal acuan kedua menjelaskan mengamankan data menggunakan enkripsi Secure Shell (SSH). Dari masalah tersebut maka FTP server dengan user dapat saling bertukar data dengan aman dalam arti meminimalisir kemungkinan kebocoran atau pembobolan data penting di jaringan, jadi pada tugas akhir ini saya akan membuat penggabungan antara kedua jurnal acuan. Di tugas akhir ini akan membuktikan pengamanan pertukaran data FTP server (Debian) dengan user (Windows) dengan menggunakan tunnel SSH yang didalam nya terdapat aktivitas FTP, serta parameter yang digunakan yaitu waktu sampai data / latency, delay dan throughput.

1.2 PERUMUSAN MASALAH

Berdasarkan latar belakang yang telah di jelaskan diatas, maka dapat dirumuskan masalah tugas akhir ini, yaitu :

1. Bagaimana cara mengamankan pertukaran data dengan menggunakan tunnel SSH?
2. Bagaimana cara melakukan pengamanan FTP server dengan menggunakan tunnel SSH?
3. Bagaimana melakukan pengujian kinerja menggunakan parameter QoS (Quality of Service) latency, delay dan throughput?

1.3 BATASAN MASALAH

Berikut ini beberapa batasan masalah dari " UJI KELAYAKAN FTP SERVER DENGAN TUNNEL SSH TERHADAP MAN IN THE MIDDLE" yaitu :

1. Menciptakan pertukaran data antara FTP server dengan user secara aman menggunakan Tunneling SSH.
2. Menghasilkan perbedaan antara pengamanan FTP standart dengan Tunneling SSH.
3. Menggunakan parameter QoS latency, delay dan throughput.
4. Untuk file yang digunakan antara 5 MB sampai dengan 5 GB.
5. Metode serangan yang digunakan adalah Man In The Middle Sniffing.

1.4 TUJUAN

Dengan mengacu pada perumusan masalah yang telah disebutkan di atas, maka tujuan yang akan dicapai dalam penyusunan tugas akhir ini sebagai berikut:

1. Menguji tingkat keamanan pada implementasi SSH dalam melindungi jalur FTP saat aktifitas pertukaran data dari berbagai kemungkinan serangan.

2. Melakukan pengujian yang berfokus pada fungsi enkripsi SSH dalam mengamankan transmisi FTP dengan menggunakan enkripsi SSH.
3. Mendapatkan kinerja pengujian dengan berdasarkan parameter delay, latency & throughput.

1.5 MANFAAT

Manfaat yang diharapkan dari tugas akhir ini adalah sebagai berikut :

1. Sebagai tunnel pengamanan FTP melalui enkripsi SSH.
2. Bermanfaat agar bisa mengenal lebih jauh tentang cara mengamankan jaringan yang baik.
3. Bermanfaat menambah informasi tentang perbedaan cara kerja FTP enkripsi SSH dan FTP tanpa menggunakan enkripsi SSH.

1.6. SISTEMATIKA PENULISAN

Dalam tugas akhir ini laporan akan dibagi menjadi 5 bab dengan sistematika penulisan sebagai berikut:

Bab I PENDAHULUAN

Berisi Latar Belakang, Perumusan Masalah, Batasan Masalah Tujuan, Manfaat, Metodologi dan Sistematika Penulisan

Bab II TINJAUAN PUSTAKA

Berisi tentang penelitian terdahulu yang sebelumnya telah dilakukan serta berisi teori-teori dan penjelasan dari metode yang akan digunakan.

Bab III METODOLOGI

Berisi tentang perencanaan serta analisis terhadap pembuatan sistem deteksi objek manusia.

Bab IV HASIL DAN PEMBAHASAN

Berisi tentang pembuatan sistem serta pengujian dan pengecekkan terhadap sistem yang telah dibuat.

Bab V PENUTUP

Berisi kesimpulan yang dapat diambil dari tugas akhir serta saran yang berguna untuk pengembangan selanjutnya.