Journal of Science and Social Research ISSN 2615 – 4307 (Print)
February 2021, IV (1): 28 - 33 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

IMPLEMENTASI SSL UNTUK PENCEGAHAN MAN IN THE MIDDLE ATTACK PADA FTP SERVER

Sahren
STMIK Royal, Kisaran
e-mail:sahren.one@gmail.com

Abstract: An advancement in communication technology currently has an influence on developments in data management in the joints of life, making the need for a media center something a must in digital archive storage. Data will not always be stored in personal computers, but it would be better if there was a centralized data container to be a solution in storage media, in order to prevent data loss or data backup. The term network (network) is used when there are at least two or more devices that are connected to one another. To carry out data exchange in this network, a protocol is used that specifies how data is exchanged, and one of the most widely used protocols is the File Transfer Protocol (FTP). The FTP protocol is not secure enough, because when data transfers there is no security to protect it and there is a very high risk of Man In The Middle Attack (MITM) or wiretapping. Therefore the FTP protocol is necessary for additional security, by implementing the SSL security protocol or Secure Socket Layer Security protecting the FTP protocol during data transfer. SSL certificates are used for the purpose of handling the security of data packets transmitted over the network system. When SSL is activated, the server and client when the connection occurs will be encrypted so that the data cannot be seen by others.
Keywords: FTP; MITM; Network; Server; SSL.

Abstrak: Suatu Kemajuan teknologi komunikasi saat ini memiliki pengaruh terhadap perkembangan didalam pengelolaan data didalam sendi kehidupan, membuat kebutuhan akan media center menjadi sesuatu yang harus dalam penyimpanan arsip digital. Data tidak selamanya akan tersimpan di dalam personal computer saja tetapi akan lebih baik jika ada wadah data terpusat menjadi solusi dalam media penyimpanan, agar menjaga dari kehilangan data atau cadangan data. Istilah jaringan (network) dipakai apabila terdapat minimal dua atau lebih perangkat yang terhubungkan satu dengan yang lainnya. Untuk melaksanakn pertukaran data didalam jaringan ini, digunakan protocol yang menspesifikasikan bagaimana data dipertukarkan, dan salah satu protocol yang banyak digunakan adalah File Transfer Protocol (FTP). FTP (File Tranfer Protocol) umumnya bermanfaat sebagai sarana pertukaran file atau data dalam suatu network. Protokol FTP tidaklah cukup aman, dikarenakan ketika transfer data tidak ada keamanan untuk melindunginya dan sangat beresiko terjadinya Man In The Middle Attack (MITM) atau penyadapan. Maka dari itu protokol FTP perlu untuk penambahan keamanan, dengan menerapkan protokol keamanan SSL atau Secure Socket Layer Security melindungi protokol FTP pada saat transfer data. Sertifikat SSL dimanfaatkan untuk keperluan menangani keamanan paket data yang ditransmisikan melalui sistem jaringan. Ketika SSL diakatifkan, maka server dan client ketika terjadi koneksi akan ter enkripsi sehingga data yang ada tidak dapat untuk dilihat oleh orang lain.
Kata kunci: FTP; MITM; Server; SSL.

PENDAHULUAN

Suatu Kemajuan teknologi komunikasi saat ini memiliki pengaruh terhadap perkembangan didalam pengelolaan data. Dimana data dari satu lokasi bisa ditransfer ke lokasi lainnya menggunakan bantuan sarana telekomunikasi.

Pengiriman data lewat komputer dilaksanakan melalui media transmisi elektronik, yang sering diartikan dengan pengistilahan komunikasi data (data communication). Istilah jaringan (network) dipakai apabila terdapat minimal dua atau lebih perangkat yang terhubungkan satu dengan yang lainnya. Untuk melaksanakn pertukaran data didalam jaringan ini, digunakan protocol yang menspesifikasikan bagaimana data dipertukarkan, dan salah satu protocol yang banyak digunakan adalah File Transfer Protocol (FTP).

File Transfer Protocol (FTP) dasarnya berguna sebagai protocol guna sarana tukar menukar files atau data didalam suatu networks yang berbasiskan koneksi TCP. FTP merupakan protocol pilihan yang paling cocok digunakan dalam save files secara cepat dan efisien dalam proses uploads dan downloads dari komputer server ke client maupun sebaliknya (Ruwaida & Kurnia, 2018). File Transfer Protocol (FTP) akan dapat diakses kapan saja selama user dapat terhubung dengan jaringan lokal maupun jaringan internet. Saat ini protocol File Transfer Protocol (FTP) menjadi rentan terhadap serangan cyber seperti Sniffing attack, Scanning, Man In The Middle Attack, DDoS dan lainnya (Khairunnisa & Sutarti, 2017). Serangan- serangan tersebut biasanya dilakukan untuk mengetahui username, password, maupun file yang di-upload atau yang di-download oleh user. Maka dari itu dibutuhkan layanan keamanan guna menjaga komunikasi antara user dengan server. File Transfer Protocol (FTP) server dapat dibekali oleh Secure Socket Layer (SSL) (Ruwaida & Kurnia, 2018). SSL dirancang untuk memberikan jaminan keamanan dan layanan kompresi ke data yang dihasilkan dari lapisan aplikasi, ini biasanya ditemukan di HTTP, sebagai keamanan data antara transport dan aplication layer (Habibi et al., 2017).

Teknologi Secure Socket Layer menggunakan konsep kriptografi kunci publik untuk bisa mencapai komunikasi yang benar-benar aman antara server dan client (Novi & Zaini, 2017). Kedua pihak yang berkomunikasi (server dan client) harus saling mengirimkan data yang disamarkan dengan teknik enkripsi, dan untuk membaca data tersebut digunakan kunci yang hanya dimiliki oleh kedua pihak yang sedang berkomunikasi saja. Sehingga apabila ada pihak lain yang mencoba untuk menyadap, data tidak akan terbaca atau tersamarkan dalam karakter yang acak.

Beberapa penelitian terdahulu telah banyak dilakukan berkaitan File Transfer Protocol (FTP) maupun penelitian yang mengkaji penggunaan Secure Socket Layer (SSL) sebagai system keamanan didalam komunikasi jaringan. (Habibi et al., 2017) melakukan penelitian untuk menganalisa protocol Secure Socket Layer terhadap dua bentuk serangan yaitu Heartbleed Bug dan Distributed Denial of Service (DDoS). (Novi & Zaini, 2017) melakukan penelitian tentang pemanfaatan Secure Socket Layer sebagai pengaman data rekam medis tumor otak dari berbagai serangan seperti sniffing selama ternjadinya pertukaran data di jaringan internet. (Ruwaida & Kurnia, 2018) melakuka penelitain untuk merancang File Transfer Protocol (FTP) dengan pengamanan open ssl pada jaringan VPN Mikrotik. (Khadafi et al., 2019) melakukan penelitian implementasi firewall dan port knocking untuk keamanan data pada FTP server yang berbasis linux ubuntu server.

Penggunaan metode File Transfer Protocol ini diharapkan dapat membantu mempermudah didalam penyimpanan files dan untuk berbagi data didalam jaringan. Selain itu penggunaan metode pengamanan dengan Secure Socket Layer bertujuan sebagai keamanan agar layanan yang ada menjadi aman dari ancaman Man In The Middle Attack (MITM). Untuk pengujian ini akan digunakan metode penyerangan MITM. Serangan MITM yang digunakan teknik sniffing.

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
February 2021, IV (1): 28 - 33 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

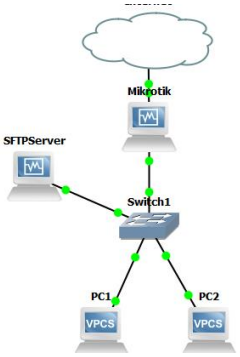
METODE

Kerangka kerja penelitian merupakan tahapan-tahapan sistematis yang dilakukan oleh penulis dalam menyelesaikan penelitian yang berhubungan dengan perancangan sistem keamanan File Trasfer Protocol (FTP) dengan Secure Socket Layer (SSL). Adapun tahapan kerja dari penelitian ini dapat dilihat pada gambar 1. berikut ini: Observasi, metode pengumpulan data melalui pendekatan ke lapangan dengan mengambil data-data yang ada di lapangan atau melakukan peninjauan secara langsung ke objek yang diteliti.

Gambar Kerangka Kerja Penelitian

HASIL DAN PEMBAHASAN

Dengan melihat permasalahan yang terjadi di Sistem Jaringan dinas pendidikan kabupaten asahan maka peneliti mengusulkan untuk membangun *Server File Transfer Protokol* yang akan mengatasi pertukaran data menggunakan perangkat eksternal, menyediakan keamanan data dan menyediakan tempat penyimpanan data yang reliable dan efisien serta memiliki sistem keamanan yang baik. Dari sistem jaringan yang berjalan pada dinas pendidikan peneliti tetap menggunakan alokasi IP Address yang sedang berjalan hanya menambahkan *IPAddress static* pada router untuk dipergunakan oleh *Server File Transfer Protocol.* Adapun topologi dari sistem yang di usulkan tertera pada Gambar 2 berikut ini.



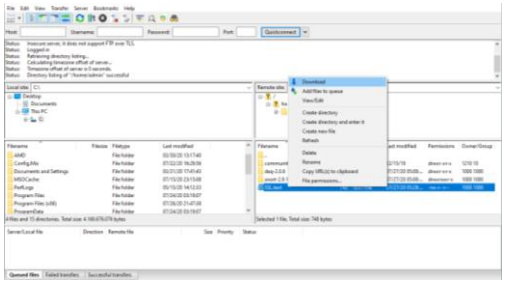
Gambar Topologi Usulan

Implementasi sistem keamanan *File Transfer Protocol* dengan *Secure Socket Layer* akan diaplikasikan pada *CentOS 7 server*. Dalam pengujian ini sistem ini diimplementasikan dalam bentuk virtualisasi menggunakan Virtual Box yang dapat dijalankan diberbagai platform sistem operasi seperti *Windows, Linux* maupun Mac OS.

Pada sistem yang dibangun akan dilakukan beberapa pengujian, ini dilakukan agar sistem yang dibuat dapat berjalan sesuai dengan kebutuhan dan tujuan dalam jurnal ini. Rangkaian pengujian yang dilakukan adalah pengujian FTP *Server* dan pengujian keamanan FTP *Server*.

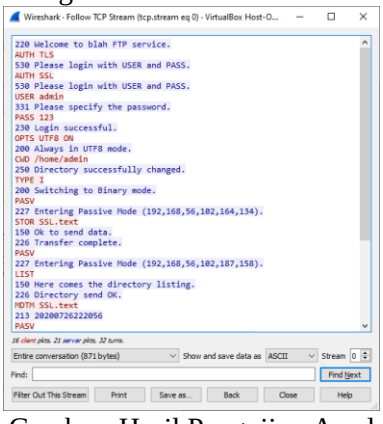
Pengujian akses FTP *server* dilakukan dengan menggunakan aplikasi khusus yaitu *file zilla*, dengan aplikasi ini user dapat dengan mudah untuk mengambil atau mendownload *file* yang ada pada *server*, sesuai dengan kebutuhan yang diinginkan. Disini user yang mengakses FTP *server* akan diminta untuk memasukkan *password* terlebih dahulu, guna keamanan akses pada FTP *server*. Setelah user berhasil login maka user dapat menggunakan FTP *server* untuk beberapa keperluan pengambilan data dari *server* maupun menyimpan data ke *server*. Pada gambar 3 disini akan dilakukan uji coba untuk mengambil data dari *server* dengan cara mendownload data yang terdapat pada salah satu directory penyimpanan pada *server*.

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
February 2021, IV (1): 28 - 33 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR



Gambar Proses *Download* File Pada FTP *Server*

Selain untuk men-download file atau dokumen pada server layanan FTP juga menyediakan fasilitas upload, sehingga user juga dapat menyimpan data atau dokumennya pada FTP *server*. Untuk layanan FTP *server* telah berjalan dengan baik maka selanjutnya perlu dilakukan uji coba terhadap kemanan dari layanan FTP server ini. Untuk menguji keamanan suatu server disini penulis mekukakan pembacan paket yang lewat didalam jaringan atau teknik ini juga biasa disebut dengan *sniffing.* Dengan teknik ini akan didapatkan sekumpulan proses komunikasi yang terjadi yaitu proses komunikasi didalam jaringan. Selanjutnya dari hasil tangkapan data tersebut dapat dilihat apakah komunikasi yang terjadi aman atau tidak. Misalnya ketika user login ke *server* FTP user dan passwordnya serta aktivitas yang dikerjakan dapat atau tidak dibaca oleh pihak ketiga.

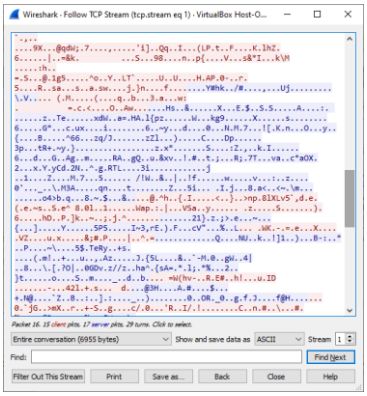


Gambar Hasil Pengujian Awal Keamanan FTP *Server*

Pada gambar dapat dilihat hasil capturing packet dengan *wireshark* pada FTP *server*, dimana dapaat dilihat sebuah fakta bahwa FTP *serve*r yang tidak dilengkapi dengan keamanan SSL dapat dilihat *packet* data yang di trasmisikan. Pada hasil *capturing packet* tersebut diperoleh hasil yaitu mendapatkan user dan *passsword* untuk admin FTP *server*. Ini terjadi dikarenakan komunikasi antara *server* dengan *client* tidak di enkripsi sehingga dengan dilakukan penyerangan dengan teknik *sniffing* paket data yang dikomunikasikan tersebut dapat dilihat. Pada tahapan ini *server* FTP sudah siap digunakan namun dalam komunikasinya belum aman sepenuhnya.

Pada layanan FTP *server* yang dibangun ini menggunakan sistem keamanan dengan menggunakan kriptografi algoritma RSA 2048 dalam bentuk *certifikat Secure Socket Layer* (SSL) yang dipasang pada *server*. Untuk pertama kali akses ke *server* FTP maka akan muncul satu *form* notifikasi yang menunjukkan terdapat *certifikate* yang tidak dikenal. disini setiap user yang menggunakan *filezilla* harus mendaftarkan *certificate* tersebut ke aplikasi yang digunakan agar layanan FTP *server*nya dapat digunakan dengan baik. setelah *verifikasi certificate* tersebut selesai barulah *user* dapat menggunakan layanan FTP *Server.*

Selanjutnya disini perlu diuji Kembali untuk tingkat keamanan dari FTP Server. Sebelumnya telah dilakukan penyadapan atau serangan packet sniffing ke FTP *Server* dari awal yaitu saat pertama login user login ke FTP *server*. Pada gambar 5 disini memperlihatkan hasil dari serangan packet *sniffing* dimana setiap data yang dikomunikasikan di FTP *Server* sudah di *enkripsi* sehingga data tidak lagi dapat disadap, di modification dan fabrication (Prabhakar, 2017).



Gambar Hasil Pengujian Keamanan FTP Server

SIMPULAN

Dari serangkaian penelitian dan hasil uji coba maka disini dapat disimpulkan bahwa Metode pengamanan dengan Secure Socket Layer (SSL) dapat di implementasikan dan berjalan dengan baik pada FTP Server. Keamanan File Transfer Protocol (FTP) dengan menggunakan Secure Socket Layer (SSL) secara standar terbukti dapat melindungi transmisi FTP Server dari Tindakan penyadapan paket data atau Man In The Middle Attack.

DAFTAR PUSTAKA

Adiguna, A. R., Saputra Chandra, M., & Pradana, F. (2018). Analisis dan Perancangan Sistem Informasi Manajemen Gudang pada PT Mitra Pinasthika Mulia Surabaya. *Pengantar Sistem Informasi*, *2*(2), 612–621. https://doi.org/10.1016/j.humimm.2008.04.008

Habibi, J. A., Munadi, R., & Yovita, L. V. (2017). Analysis secure socket layer protocol with heartbleed bug and distributed denial-of-service. *ICCEREC 2016 - International Conference on Control, Electronics, Renewable Energy, and Communications 2016, Conference Proceedings*, 54–59. https://doi.org/10.1109/ICCEREC.2016.7814960

Khadafi, S., Nurmuslimah, S., & Anggakusuma, F. K. (2019). *Implementasi Firewall Dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server*. *4*(3), 181–188.

Khairunnisa, & Sutarti. (2017). Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan Ddos (Distributed Denial of Service) Berbasis Honeypot. *Jurnal PROSISKO*, *4*(2), 8.

Kurniawan, B., & Herryanto, D. (2017). Perancangan Dan Implementasi Data Center Menggunakan File Transfer Protocol (Ftp). *Perancangan Dan Implementasi Data Center Menggunakan File Transfer Protocol (Ftp)*, *2*(2), 91–97. https://doi.org/10.1360/zd-2013-43-6-1064

Novi, N., & Zaini, Z. (2017). Secure Socket Layer untuk Keamanan Data Rekam Medis Tumor Otak pada Health Information System. *Jurnal Nasional Teknik Elektro*, *6*(3), 137. https://doi.org/10.25077/jnte.v6n3.405.2017

Prabhakar, S. (2017). *Research in Computer Applications and Robotics Network Security in Digitalization : Attacks and*. *5*(5), 46–52.

Ruwaida, D., & Kurnia, D. (2018). Rancang Bangun File Transfer Protocol (Ftp) Dengan Pengamanan Open Ssl Pada Jaringan Vpn Mikrotik Di Smk Dwiwarna. *Computer Engineering, Science and System Journal*, *3*(1), 45. https://doi.org/10.24114/cess.v3i1.8267

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
February 2021, IV (1): 28 - 33 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR