TELCOMATICS, Vol.5 No.1, Desember 2020, pp. 12-18
eISSN: 2541-5867
DOI: 10.37253/telcomatics.v5i1.851

Analisis Keamanan FTP server Menggunakan Serangan Man-In-The-Middle Attack

Zulkarnain
Sistem Informasi, Ilmu Komputer, Universitas Internasional Batam, Jl. Gajah Mada, Batam, 29442, Indonesia
E-mail: zulkarnain@uib.ac.id

Abstrak

FTP merupakan metode pilihan yang tepat dalam penyimpanan dengan kecepatan transfer yang lebih baik, akan tetapi seiring perkembangan teknologi semakin banyak tools yang dapat melakukan tindak kejahatan diantaranya melakukan sniffing. Sniffing merupakan tindkan hacking paling mudah dan paling sulit untuk diantisipasi, dengan berbagai macam tool yang dapat digunakan dan bersifat free, yang dapat membahayakan user yang tidak teliti atau tidak mengerti sepenuhnya tentang kemanan jaringan computer. Dalam Transfer file, Protocol Transport merupakan bagian yang sangat penting. Transport layer didisain untuk komunikasi terminal diantara aplikasi yang berjalan pada host-host yang berbeda. Dengan menggunakan FTP, user dapat memanipulasi file komputer lain seolah-olah di komputer sendiri. FTP hanya berjalan secara ekslusif di jaringan TCP. Secara default, FTP server akan melakukan listening pada port 21 untuk mendeteksi adanya permintaan koneksi dari FTP client. Agar User dapat terlindung dari serangan sniffing maka dibutuhkan Protokol FTPS dimana terdapat penggabungan antara protokol FTP dan aplikasi OpenSSL. OpenSSL berfungsi untuk melindungi data user dan password melalui enkripsi berupa berkas sertifikat. Setelah melakukan pengujian hal tersebut dapat dihindari dengan dengan menggunakan FTPS. Ketika pengguna akan login memasukkan user name dan password maka protokol FTPS akan melakukan enkripsi data, sehingga informasi user dan password di jaringan sulit untuk disadap oleh aplikasi-aplikasi sniffer yang banyak beredar di internet salah satunya seperti cain & abel.
***Katakunci**: Jaringan Komputer, Keamanan Jaringan Komputer, FTP, FTPS, SSL*

Abstract

FTP is an appropriate method of storage with better transfer speeds, but as technology develops more tools can commit crimes including sniffing. Sniffing is the easiest and most difficult hacking to anticipate, with a variety of tools that can be used and are free, which can endanger users who are not thorough or do not fully understand about the security of computer networks. In file transfer, Protocol Transport is a very important part. The transport layer is designed for terminal communication between applications running on different hosts. By using FTP, users can manipulate other computer files as if on their own computer. FTP only runs exclusively on TCP networks. By default, the FTP server will listen on port 21 to detect connection requests from the FTP client. So that Users can be protected from sniffing attacks, FTPS Protocol is needed where there is a merging between the FTP protocol and OpenSSL applications. OpenSSL functions to protect user data and passwords through encryption in the form of certificate files. After testing it can be avoided by using FTPS. When the user will log in, enter the user name and password, then the FTPS protocol will encrypt the data, so that user and password information on the network is difficult to be tapped by sniffer applications that are widely circulated on the internet, one of them is cain & abel.
***Keywords**: Computer Network, Computer Network Security, FTP, FTPS, SSL*

I. LATAR BELAKANG

Dewasa ini kita menyadari bahwa informasi merupakan suatu kebutuhan yang tidak bisa dipandang sebelah mata lagi, mengingat pentingnya sebuah informasi pada saat ini. Terlebih lagi dengan informasi, seseorang akan bisa memiliki wawasan serta ilmu pengetahuan yang luas. Begitu banyak media informasi yang telah beredar pada saat ini, sehingga memudahkan kita untuk memperoleh informasi dengan sangat cepat [1].

Hal ini tidak terlepas dari peranan media Internet yang menyediakan fasilitas untuk melakukan pertukaran data melalui File Transfer Protocol (FTP). *File Transfer Protocol* menjadi banyak digunakan karena kemudahan penggunaannya untuk proses pertukaran data. *File Transfer Protocol* (FTP) tidak hanya digunakan sebagai media pertukaran data antar komputer, tetapi juga dapat digunakan untuk pertukaran data antara server dengan client [2], [3].

eISSN: 2541-5867
DOI: 10.37253/telcomatics.v5i1.851

Dalam Transfer file, *Protocol Transport* merupakan bagian yang sangat penting. *Transport layer* didisain untuk komunikasi terminal diantara aplikasi yang berjalan pada host-host yang berbeda [4]. FTP (*File Transfer Protocol*) digunakan untuk memindahkan file yang menggunakan jaringan TCP/IP. Dengan menggunakan FTP, user dapat memanipulasi file komputer lain seolah-olah di komputer sendiri. FTP hanya berjalan secara ekslusif di jaringan TCP.

Secara default, FTP server akan melakukan listening pada port 21 untuk mendeteksi adanya permintaan koneksi dari FTP client. FTP menggunakan kontrol out-of-band yang artinya FTP menggunakan koneksi yang berbeda untuk mengontrol dan untuk data. FTP bisa berjalan diberbagai jenis sistem operasi seperti Windows dan Linux yang membedakannya adalah konfigurasi. Tingkat kerumitan adalah hal yang relatif dalam konfigurasi disetiap sistem operasi yang digunakan, efisiensi dari segi ekonomi dan keamanan [4], [5].

FTP merupakan metode pilihan yang tepat dalam penyimpanan dengan kecepatan transfer yang lebih baik, akan tetapi seiring perkembangan teknologi semakin banyak tools yang dapat melakukan tindak kejahatan diantaranya melakukan sniffing. Sniffing merupakan tindkan hacking paling mudah dan paling sulit untuk diantisipasi, dengan berbagai macam tool yang dapat digunakan dan bersifat free, yang dapat membahayakan user yang tidak teliti atau tidak mengerti sepenuhnya tentang keamanan jaringan computer [6]. Sehingga jika dilihat dari segi keamanan protokol FTP tidak mendukung enkripsi data user dan password pengguna ketika login kedalam server FTP. Kelemahan FTP ketika user dan password digunakan pada saat login, user dan password tersebut sangat mudah disadap / sniffing didalam jaringan dalam kondisi tidak terenkripsi [7].

Protokol SFTP terdapat penggabungan antara protokol FTP dan aplikasi OpenSSL, dimana OpenSSL berfungsi untuk melindungi data user dan password melalui enkripsi berupa berkas sertifikat. Ketika pengguna akan login memasukkan user name dan password maka protokol SFTP akan melakukan enkripsi data, sehingga informasi user dan password di jaringan sulit untuk disadap oleh aplikasi-aplikasi sniffer yang banyak beredar di internet salah satunya seperti cain & abel. Pada penelitian ini selain dari sisi keamana, akan membahas performance kedua protokol tersebut pada kecepatan transfer file / transfer rate kemudian melihat sumber daya CPU dan memory seberapa besar terpakai pada saat proses kerja berlangsung. Sehingga penulis mengambil judul "Analisa Performance dan Keamanan FTP Server Menggunakan Serangan Man-In-The-Middle Attack".

II. KERANGKA TEORI

File transfer protokol merupakan salah satu sarana untuk melakukan sharing file yang akan disimpan pada satu direktori pada komputer server yang di akses sejumlah besar komputer secara bersamaan. Apabilah file yang akan disharing merupakan file tertentu memerlukan autentikasi username dan pasword saat mengakses data yang disharing, secara default autentikasi pada FTP menggunakan ASCII dimana saat terjadi proses autentikasi dari komputer klien ke server tidak dilakukan engkripsi dan masih berupa plaintext.

FTP merupakan protokol di internet yang berjalan di layer aplikasi untuk melakukan transfer data atau file antara komputer dalam sebuah jaringan. Untuk itu dilakukan penerapan FTP server dan autentikasi menggunakan secure socket layer dan secure shell, sehingga proses autentikasi pada FTP server akan di engkripsi. FTPS merupakan FTP server yang menggunakan protokol SSL, sedangkan SFTP menggunakan SSH [8].

Proses autentikasi dan transfer data pada FTP tampa ssl tidak aman karena dapat ditangkap oleh tools wiresahrk. Dengan menggunakan ssl proses autentikasi dan transfer data akan melakukan engkripsi sehingga sehingga paket data yang dikirim tidak terbaca oleh tools seperti wireshark [9].

Menurut [10], sekarang ini host dalam jaringan menghadapi masalah yang lebih serius dari penyerang. Seorang penyerang mencoba melakukan hack pada IP dan alamat MAC, melihat koneksi, memanipulasi informasi dan memutuskan hubungan antara host. Penyerang mengubah informasi di ARP tabel untuk menangkap informasi dari host. Sebelumnya banyak alat yang digunakan untuk mengeksploitasi kerentanan di ARP, tapi semua alat ini memanfaatkan kelemahan dari protokol

TELCOMATICS, Vol.5 No.1, Desember 2020, pp. 12-18
eISSN: 2541-5867
DOI: 10.37253/telcomatics.v5i1.851

ARP itu sendiri, jika kita mengubah definisi protokol ARP itu akan menciptakan masalah kompatibilitas yang lebih serius dan tidak dapat diterima.

Protokol ARP adalah keluarga protokol IP/TCP. Untuk tujuan ini, tabel ARP dibangun untuk memetakan alamat MAC untuk setiap alamat IP. Ketika permintaan dibuat untuk paket yang akan disampaikan, ARP pertama berkonsultasi pada tabel untuk menentukan apakah alamat MAC untuk alamat IP tujuan sudah ditentukan.[11]

Dengan demikian, *table list* membantu dalam mempercepat respon terhadap permintaan. Jika tidak ada entri yang ditemukan sesuai dengan alamat IP dalam tabel, maka alamat MAC ditentukan oleh protokol, dan tabel ARP diperbarui. Secara default, sebagian besar entri dalam tabel ARP bersifat dinamis. Hal ini memungkinkan sistem untuk menjadi fleksibel, misalnya mesin mengakses jaringan dengan alamat IP yang berbeda dari yang sudah disimpan dalam tabel ARP, atau jika suatu jaringan ulang, maka sifat dinamis dari tabel ARP memungkinkan benar alamat MAC harus diperbarui sesuai dengan alamat IP mereka. Namun, sifat tabel ARP ini dapat dimanfaatkan oleh cracker untuk serangan spoofing, poisoning, termasuk Man in the Middle Attack dan Denial of Service. Sebuah alat yang populer untuk tujuan ini adalah NetCut [12].

Dalam medeteksi deteksi serangan poisoning MAC terdeteksi dengan mengirimkan permintaan Inverse ARP untuk alamat MAC. Tanggapan yang diterima dapat digunakan untuk menentukan apakah komputer tersebut melakukan kloning. Tapi solusi ini sangat terbatas karena hanya mendeteksi jenis serangan ARP. Dengan keamanan port, serangan kloning dapat dicegah. Metode ini efektif tetapi gagal dalam jenis lain dari serangan ARP yang tidak memerlukan kloning alamat MAC. [13] membahas tentang pendekatan middleware untuk asynchronous serta untuk deteksi kompatibel ke belakang dan pencegahan serangan ARP cache poisoning. Namun skema ini tidak efektif jika tuan rumah sedang dalam pemalsuan down atau sedang tertutup. [14] mengusulkan mekanisme ringan dengan menggunakan tabel transisi static untuk mendeteksi ARP spoofing respon bit itu tidak memberikan solusi terhadap serangan. [15] mengusulkan mekanisme pertahanan terhadap serangan ARP yang didasarkan pada pemeriksaan paket ARP dengan menggunakan RAW pemrograman socket. [16] menggunakan static entri IP-MAC pasangan untuk setiap host di jaringan. Sistem administrator mempertahankan entri ini tetapi semacam ini jaringan gagal untuk organisasi besar. [17] mengusulkan Secure-ARP (SARP) protokol baru di mana distribusi key, key public dan private untuk menandatangani setiap pesan ARP telah digunakan. Server terpisah telah untuk menyelesaikan permintaan ARP didasarkan pada secrete sharing concept.

ARP (Address Resolution Protocol) adalah sebuah protocol pada jaringan komputer untuk menentukan jaringan host link layer mengatasi ketika hanya lapisan Internet (IP) atau network layer alamat dikenal. ARP spoofing adalah teknik yang digunakan untuk menyerang jaringan kabel atau nirkabel Ethernet. Hal ini juga dikenal sebagai ARP flooding, ARP poisoning. ARP spoofing dapat memungkinkan seorang penyerang untuk melakukan sniffing data pada frame jaringan area lokal (LAN), memodifikasi lalu lintas, atau menghentikan lalu lintas sama sekali. Prinsip ARP spoofing adalah dengan mengirim pesan ARP palsu ke Ethernet LAN. Dalam peneitian ini, kami menyajikan pendekatan baru yang merupakan perpanjangan dari ARP asli yang muncul pada tahun 1982, di mana kita merasa bahwa jika dalam sebuah jaringan, ketika sebuah node berkomunikasi mengidentifikasi benar MAC alamat dari IP tertentu alamat melalui permintaan dan mekanisme respon, itu dibuat untuk menyimpan bahwa dalam IP/MAC address pemetaan tabel untuk keseluruhan untuk host yang hidup. Dengan demikina maka dapat melakukan Man-In-The-Middle (MITM) serangan untuk alamat IP. Skema yang diusulkan berjalan lebih jauh dengan memperhatikan pertimbangan probabilitas berdasarkan mekanisme resolusi suara untuk IP baru alamat berbasis kompatibel dengan yang ada ARP [18].

File Transfer Protocol adalah sebuah protokol Internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pengiriman berkas (*file*) komputer antar mesin-mesin dalam sebuah jaringan. FTP merupakan salah satu protokol Internet yang paling awal dikembangkan, dan masih digunakan hingga saat ini untuk melakukan pengunduhan (*download*) dan penggugahan (upload) berkas-

eISSN: 2541-5867
DOI: 10.37253/telcomatics.v5i1.851

berkas komputer antara klien FTP dan server FTP. Sebuah Klien FTP merupakan aplikasi yang dapat mengeluarkan perintah-perintah FTP ke sebuah server FTP, sementara server FTP adalah sebuah Windows Service atau daemon yang berjalan di atas sebuah komputer yang merespons perintah-perintah dari sebuah klien FTP. Perintah-perintah FTP dapat digunakan untuk mengubah direktori, mengubah modus pengiriman antara biner dan ASCII, menggugah berkas komputer ke server FTP, serta mengunduh berkas dari server FTP. Sebuah server FTP diakses dengan menggunakan Universal Resource Identifier (URI) dengan menggunakan format ftp://namaserver. Klien FTP dapat menghubungi server FTP dengan membuka URI tersebut [2], [4].

FTP menggunakan protokol *Transmission Control Protocol* (TCP) untuk komunikasi data antara klien dan server, sehingga di antara kedua komponen tersebut akan dibuatlah sebuah sesi komunikasi sebelum pengiriman data dimulai. Sebelum membuat koneksi, port TCP nomor 21 di sisi server akan "mendengarkan" percobaan koneksi dari sebuah klien FTP dan kemudian akan digunakan sebagai port pengatur (control port) untuk membuat sebuah koneksi antara klien dan server, untuk mengizinkan klien untuk mengirimkan sebuah perintah FTP kepada server dan juga mengembalikan respons server ke perintah tersebut. Sekali koneksi kontrol telah dibuat, maka server akan mulai membuka port TCP nomor 20 untuk membentuk sebuah koneksi baru dengan klien untuk mengirim data aktual yang sedang dipertukarkan saat melakukan pengunduhan dan penggugahan [2].

FTP hanya menggunakan metode autentikasi standar, yakni menggunakan username dan password yang dikirim dalam bentuk tidak terenkripsi. Pengguna terdaftar dapat menggunakan username dan password-nya untuk mengakses, men-*download*, dan meng-upload berkas-berkas yang ia kehendaki. Umumnya, para pengguna terdaftar memiliki akses penuh terhadap beberapa direktori, sehingga mereka dapat membuat berkas, membuat direktori, dan bahkan menghapus berkas. Pengguna yang belum terdaftar dapat juga menggunakan metode anonymous login, yakni dengan menggunakan nama pengguna anonymous dan password yang diisi dengan menggunakan alamat e-mail.

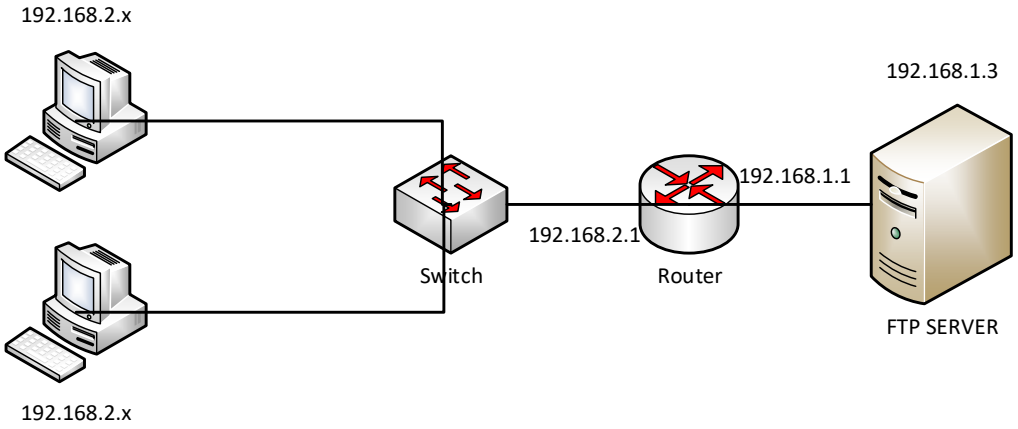
SSL atau Secure Sockets Layer adalah sebuah protokol keamanan data yang digunakan untuk menjaga pengiriman data web server dan pengguna situs web tersebut. Jenis SSL yang paling aman dapat dilihat dari tingkat keamanan SSL, yang terletak pada kekuatan enkripsi yang didukungnya (misalnya 256 bit). Semakin besar tingkat enkripsi semakin susah untuk dibobol. Secara teknis, semua SSL dengan tingkat enkripsi yang sama, mempunyai tingkat keamanan yang sama. Untuk mengetahui apabila transaksi diamankan oleh SSL adalah sebuah icon berlambangkan gembok yang terkunci akan muncul di browser yang telah diamankan dengan SSL[8], [18].

Sertifikat SSL memastikan data transaksi yang terjadi secara online di enkripsi/acak sehingga tidak dapat dibaca oleh pihak lain. Kegunaan utamanya adalah untuk menjaga keamanan dan kerahasiaan data ketika melakukan transaksi. Sertifikat SSL memberikan jaminan keamanan pada pemilik dan pengunjung situs atas data yang dikirim lewat web. Sertifikat SSL yang sering digunakan dapat dilihat pada situs perbankan untuk melakukan transaksi e-banking [19].

Man, in the middle attack (MITM) adalah serangan di mana attacker berada di tengah, bebas mendengarkan dan mengubah percakapan antara dua pihak. Serangan Man in the middle merupakan suatu tipe serangan yang memanfaatkan kelemahan Internet Protocol (ip). Serangan MITM adalah bentuk aktif menguping dimana penyerang membuat koneksi independen dengan korban dan pesan relay antara mereka, membuat mereka percaya bahwa mereka berbicara langsung satu sama lain melalui koneksi pribadi, padahal sebenarnya seluruh percakapan dikendalikan oleh penyerang. Penyerang harus mampu mencegat semua pesan terjadi antara kedua korban dan menyuntikkan yang baru, misalnya, seorang penyerang dalam jangkaun penerimaan terenskripsi Wi-Fi jalur akses nirkabel, dapat menyisipkan dirinya sebagai seorang Man-In-The-Middle [18].

Konsep dasar serangan ini secara umum adalah penyerang berada ditengah – tengah atau di antara dua komputer yang sedang berkomunikasi, sehingga secara teknis memungkinkan penyerang untuk melihat, mengubah dan mengontrol data yang dikirim antar dua komputer tersebut, namun rute paket

TELCOMATICS, Vol.5 No.1, Desember 2020, pp. 12-18
eISSN: 2541-5867
DOI: 10.37253/telcomatics.v5i1.851



Gambar 1: Rancangan penelitian

yang dikirimkan atau ditunjukkan kepada host lain harus melalui mesin penyerang.

Ada berbagai teknik dan istilah salam serangan Man in the middle, Antara lain adalah:

1. *Sniffer*
   Sniffer yang juga dikenal sebagai *Network Analyzer* atau *Ethernet Sniffer* ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Dikarenakan data mengalir secara bolak–balik ada jaringan, aplikasi ini menangkap tiap–tiap paket dan kadang – kadang menguraikan isi dari RFC (*Request for Comments*) atau spesifikasi yang lain.

2. *Spoofing*
   Spoofing adalah situasi dimana seseorang berhasil menyamar sebagai user dengan memalsukan data dengan demikian mendapatkan keuntungan tidak sah.

3. *Interception*
   Interception merupakan ancaman terhadap *secrecy*, dimana orang yang tidak berhak namun berhasil mendapatkan akses informasi dari dalam sistem komputer.

4. *Modification*
   Modification merupakan ancaman terhadap intergrity dimana orang yang tidak berhak dapat mengakses maupun merubah suatu informasi.

5. *Fabrication*
   Fabrication adalah teknik menambahkan objek atau informasi palsu pada informasi yang asli, sehingga data atau informasi berubah.

III. HASIL PENELITIAN

Pada penelitaian ini akan menggunakan mikrotik Windows Server 2008 sebagai FTP server, dan windows 8 sebagai klien, dan 1unit router mikrotik sebagai penghubung antara server dan klien. Adapun perancangannya serperti pada Gambar 1.

Untuk komputer user masing-masing mendapatkan IP address secara DHCP. Untuk men-setting IP pada komputer, langkah-langkah yang harus dilakukan adalah pilih Start Menu, Control Panel, Network and Internet, Network Connection, Local Area Connection Properties, Internet Protokol Version 4.

Pada pengujian ini terdapat dua laptop yang terhubung ke jaringan LAN, satu laptop client (korban) dan satu laptop attecker (penyerang). Dimana korban akan mengakses FTP Server dan penyerang akan *Sniffing* guna mendapatkan *username* dan *password* korban.

1. Semua sudah terhubung dalam jaringan, penyerang akan melakukan sniffing menggunakan cain & abel.
2. Pada menu bar yang ada pilih sniffing, kemudian dan Add (+) untuk melakukan scanning maka akan muncul gambar

eISSN: 2541-5867
DOI: 10.37253/telcomatics.v5i1.851

seperti dibawa ini. Disini kita akan memasukkan range jaringan LAN yang akan kita sniffing

3. Setelah melakukan scan maka akan muncul IP address yang telah discan tersebut.
4. Langkah berikutnya adalah melakukan ARP poisoning agar user yang terhung ke server akan melalui computer penyerang. Pada menu pilih ARP kemudian Add, maka akan muncul tampilan seperti pada gambar dibawa ini, makan kita akan memilih IP korban.
5. Sekarang kita akan melakukan pada sisi user, disini kita akan menggunakan WinSCP sebagai FTP klient untuk logic ke Server. Host name adalah alamat server, file protocol FTP, pada bagian encryption di isi no encryption, dan usernamae password.
6. Setelah berhasil login dan masuk ke FTP Server, maka kita akan melihat di computer penyerang apakah username dan password dapat di sniffing. Sekarang kita masuk ke cain & abel, masuk ke menu ARP dan pilih Password. Disini kita dapat melihat apabilah pada saat Login tidak menggunakan encryption maka username dan password akan terbaca oleh penyerang.

Setelah menerapkan sistem keamanan pada FTP Server maka kita akan melakkan pengujian sama seperti pada saat belum menggunakan SSL/TLS. Yang membedakan disini adalah dimana pada saat Login ke server, user akan menggunakan encryption yaitu explicit SSL/TLS atau implicit SSL/TLS. *Encryption implicit* SSL/TLS akan menggunakan special port yaitu 990 sedangkan encryption explicit akan tetap menggunakan port 21.

Setelah berhasil login dan masuk ke FTP Server dengan implicit SSL/TLS, maka kita akan melihat di computer penyerang apakah username dan password dapat di sniffing. Sekarang kita masuk ke cain & abel, masuk ke menu ARP dan pilih Password. Disini kita tidak dapat melihat atau menagkap username dan password klien. Kita akan melakukan percobaan kedua yaitu dengan menggunakan encryption expilicit SSL/TLS. Sama seperti sebelumnya kita akan login ke server.

Setelah berhasil login dan masuk ke FTP Server dengan explicit SSL/TLS, maka kita akan melihat di computer penyerang apakah username dan password dapat di sniffing. Sekarang kita masuk ke cain & abel, masuk ke menu ARP dan pilih Password. Disini kita tidak dapat melihat atau menagkap username dan password klien.

IV. PEMBAHASAN

Berdasarkan hasil penelitian yang telah dilakukan dengan menggunakan encryption makan data akan aman, dan terbebas dari sniffing. Ini disebapkan karena adanya protocol SSL atau Secure Sockets Layer. Secure Sockets Layer (SSL) merupakan sistem yang digunakan untuk mengenkripsi pengiriman informasi pada jaringan komputer, sehingga data dapat dikirim dengan aman. Protokol SSL mengatur keamanan dan integritas menggunakan enkripsi, autentikasi, dan kode autentikasi pesan. SSL protocol menyedian privasi komunikasi di jaringan komputer. SSL tidak mendukung fileencryption, access-control, atau proteksi virus, jadi SSL tidak dapat membantu mengatur data sensitif setelah dan sebelum pengiriman yang aman. Protokol SSL terdiri dari dua sub-protokol: SSL record protocol dan SSL handshake protocol. SSL record protocol mendefinisikan format yang digunakan untuk mentransmisikan data. Sedangkan SSL handshake protocol melibatkan SSL record protocol untuk menukarkan serangkaian pesan antara SSL enabled server dan SSL enable client ketika keduanya pertama kali melakukan koneksi SSL. Pertukaran pesan tersebut digunakan untuk memfasilitasi tindakan sebagai berikut:

1. Autentikasi dari server ke klien
2. Mengizinkan klien dan server untuk memilih algoritma kriptografi atau sandi, yang mendukung komunikasi keduanya.
3. Autentikasi dari klien ke server.
4. Menggunakan teknik enkripsi public key untuk membuka data yang dienkripsi.
5. Membuat enkripsi koneksi SSL

V. KESIMPULAN

Berdasarkan pengujian yang telah dilakukan dapat diambil kesimpulan bahwa tampa adanya sistem keamanan pada suatu jaringan komputer maka akan merepotkan user-user yang terhubung di jaringan tersebut. Secara tidak

TELCOMATICS, Vol.5 No.1, Desember 2020, pp. 12-18
eISSN: 2541-5867
DOI: 10.37253/telcomatics.v5i1.851

sadar serangan seperti sniffing bias saja terjadi dan datang dari mana saja, baik itu user yang tidak dikenal maupun teman sendiri, baik itu untuk kepentingan pribadi maupun hanya sekedar iseng/jail. Serangan yang sering dilakukan pada jaringan LAN yaitu Sniffing dengan menggunakan Cain & Abel, namun hal tersebut dapat dihindari dengan memanfaatkan dengan meningkatkan system keamanan pada pada sisi Server dengan menerapakan protol SSL/TLS sehingga pada saat melakukan autentikasi ke server data dalam keadaan terenkripsi.

Untuk kedepannya, selaian menerapankan system keamana pada sisi server kita juga harus meningkatkan system keamana pada jaringan LAN, sehingga tidak ada proses sniffing pada jaringan tersebut. Meskipun SSL suda secure, tetapi masih bias di jebol dengan memalsukan sertificate untuk autentikasi pada server, namu hal tersebut masi sulit dilakukan kecuali orang-orang yang sudah ahli dibidang hacking.

VI. DAFTAR PUSTAKA

[1] F. Mahdia and F. Noviyanto, "Pemanfaatan Google Maps API Untuk Pembanguan Sistem Informasi Manajemen Bantuan Logistik Pasca Bencana Alam Berbasis Mobile Web," J. Sarj. Tek. Inform., vol. 1, no. 1, 2013.

[2] A. F. Oklilas and B. Rawan, "Implementasi FTP Server dengan Metode Transfer Layer Security untuk Keamanan Transfer Data Menggunakan CentOS 5.8," J. Generic, vol. 9, no. 2, pp. 348–355, 2014.

[3] F. Hariadi, "Pembuatan Sistem Informasi Perpustakaan Pada SDN Sukoharjo Pacitan Berbasis Web," IJNS-Indonesian J. Netw. Secur., vol. 2, no. 4, 2012.

[4] Y. L. Oktavianus, "Membangun Sistem Cloud Computing Dengan Implementasi Load Balancing dan Pengujian Algoritma Penjadwalan Linux Virtual Server Pada FTP Server," J. Nas. Tek. Elektro, vol. 2, no. 1, 2013.

[5] D. Lukitasari and A. F. Oklilas, "Analisis Perbandingan Load Balancing Web Server Tunggal Dengan Web server Cluster Menggunakan Linux Virtual Server," J. generic, vol. 5, no. 2, 2013.

[6] D. Schneider, "The state of network security.," Netw. Secur., vol. 1, no. 1, 2012.

[7] M. M. Mustofa and E. Aribowo, "Penerapan Sistem Keamanan Honeypot Dan IDS Pada Jaringan Nirkabel (Hotspot)," J. Sarj. Tek. Inform., vol. 1, no. 1, 2013.

[8] R. Cheema and A. Gulati, "Improving the Secure Socket Layer by modifying the RSA algorithm," Int. J. Comput. Sci. Eng. Appl., vol. 2, no. 3, p. 79, 2012.

[9] P. Asrodia and H. Patel, "Network traffic analysis using packet sniffer," Int. J. Eng. Res. Appl., vol. 2, no. 3, pp. 854–856, 2012.

[10] I. B. V. H. Manuaba, R. Hidayat, and S. S. Kusumawardani, "Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus: Kantor Pusat Fakultas Teknik Universitas Gadjah Mada)," J. Nas. Tek. Elektro dan Teknol. Inf., vol. 1, no. 1, 2012.

[11] A. Amarudin, W. Widyawan, and W. Najib, "Analisis Keamanan Jaringan Single Sign On (SSO) Dengan Lightweight Directory Access Protocol (LDAP) Menggunakan Metode MITMA," SEMNASTEKNOMEDIA ONLINE, vol. 2, no. 1, 2014.

[12] D. Sharma, O. Khan, K. Aggarwal, and P. Vaidya, "A New Approach to Prevent ARP Spoofing," in Proceedings of International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2013.

[13] Y. Yang, Y. Huang, J. Cao, X. Ma, and J. Lu, "Formal specification and runtime detection of dynamic properties in asynchronous pervasive computing environments," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 8, pp. 1546–1555, 2013.

[14] S. Kumar and S. Tapaswi, "A centralized detection and prevention technique against ARP poisoning. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)," in 2012 International Conference IEEE., 2012.

[15] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya, and J. K. Kalita, "Network attacks: Taxonomy, tools and systems," J. Netw. Comput. Appl., vol. 40, no. 1, pp. 307–324, 2014.

[16] A. Wang, M. Iyer, R. Dutta, G. N. Rouskas, and I. Baldine, "Network virtualization: Technologies, perspectives, and frontiers," J. Light. Technol., vol. 31, no. 4, pp. 523–537, 2013.

[17] N. Saputro and K. Akkaya, "An Efficient and Secure ARP for Large-Scale IEEE 802.11 s-based Smart Grid Networks.," in International Conference on Ad Hoc Networks, 2013, pp. 214–228.

[18] P. K. Pateriya and S. S. Kumar, "Analysis on Man in the Middle Attack on SSL," Analysis, vol. 45, no. 23, 2012.

[19] K. Peng, "A secure network for mobile wireless service," J. Inf. Process. Syst., vol. 9, no. 2, pp. 247–258, 2013.