



**ANALISIS KEAMANAN FTP SERVER DENGAN PROTOKOL SSL DARI
SERANGAN BRUTE FORCE**

**Disusun dan Disajikan Untuk Memenuhi Persyaratan Ujian Akhir
Memperoleh Gelar Sarjana Komputer Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi
Medan**

SKRIPSI

OLEH

**NAMA : DEVI RUWAIDA
NPM : 1514370687
PROGRAM STUDI : SISTEM KOMPUTER**

**FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019**

ABSTRAK

DEVI RUWAIDA

**Analisis Keamanan FTP Server Dengan Protokol SSL Dari
Serangan Brute Force
2019**

File Transfer Protocol (FTP) Server merupakan jenis sistem yang menghubungkan hak pengakses (*client*) dan penyedia (*server*) melakukan pertukaran data yang melewati port 21. Dengan proses kerja dari *File Transfer Protocol* (FTP) yaitu pengirim (*Upload*) proses ini dilakukan dengan mengirim data dari user atau komputer client kepada penyedia FTP server adalah komputer server dan proses meminta (*Download*) dilakukan dengan user atau komputer client melakukan pengambilan atau meminta data yang disediakan oleh komputer server. *File Transfer Protocol* (FTP) server membutuhkan *Secure Socket Layer* (SSL) untuk mengamankan dalam komunikasi pertukaran data sebab FTP yang digunakan tanpa adanya SSL beresiko tidak aman, FTP bekerja dengan *transparent* dalam melakukan pertukaran data tanpa adanya proses enkripsi didalamnya. Sehingga akan beresiko terjadinya penyerangan yang merugikan pihak penyedia FTP server itu sendiri. Dengan FTP yang bekerja secara transparan akan memicu sebagian orang untuk melakukan penyerangan yaitu serangan Brute Force yang penyerangannya dilakukan dengan mencoba kemungkinan yang ada dalam mendapatkan *password* pengguna FTP.

Kata Kunci: *File Transfer Protocol* (FTP), *Secure Socket Layer*, *Brute Force*.

DAFTAR ISI

| | |
|---|----|
| ABSTRAK | |
| KATA PENGANTAR | i |
| DAFTAR ISI | ii |
| DAFTAR GAMBAR | iv |
| DAFTAR TABEL | v |
| DAFTAR LAMPIRAN | vi |
| | |
| BAB I PENDAHULUAN | |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 3 |
| 1.3 Batasan Masalah..... | 3 |
| 1.4 Tujuan Penelitian | 4 |
| 1.5 Manfaat Penelitian | 4 |
| | |
| BAB II LANDASAN TEORI | |
| 2.1 Defenisi Keamanan Jaringan..... | 5 |
| 2.2 Jaringan Komputer | 5 |
| 2.3 Topologi Jaringan..... | 7 |
| 2.4 Transmission Control Protocol/Internet Protocol (TCP/IP)..... | 12 |
| 2.5 FTP Server dan FTP Client | 13 |
| 2.6 Protokol SSL | 14 |
| 2.7 Brute Force Attack | 15 |
| 2.8 Linux | 16 |
| 2.9 Wireshark | 18 |
| 2.10 Sistem Operasi Ubuntu | 19 |
| 2.11 Virtual Box..... | 21 |
| 2.12 Flowchart | 24 |
| | |
| BAB III ANALISIS DAN PERANCANGAN SISTEM | |
| 3.1 Tahap Penelitian..... | 26 |
| 3.2 Metode Pengumpulan Data | 26 |
| 3.3 Analisis Sistem Sedang Berjalan | 27 |
| 3.4 Rancangan Penelitian | 33 |
| 3.4.1 Anggaran Biaya..... | 35 |
| 3.4.2 FTP Server dengan protocol SSL yang akan diterapkan | 36 |
| 3.4.3 Instalasi Ubuntu | 38 |
| 3.4.4 Konfigurasi Alamat IP dan NAT | 38 |
| 3.4.5 Instalasi Packet FTP Server dengan SSL..... | 40 |
| 3.4.6 Konfigurasi FTP server | 41 |
| 3.4.7 Konfigurasi SSL dan Sertifikast SSL..... | 41 |
| 3.4.8 Pengujian..... | 43 |
| | |
| BAB IV IMPLEMENTASI DAN PENGUJIAN | |
| 4.1 Kebutuhan Spesifikasi Hardware dan Software..... | 46 |

| | | |
|-------|--|----|
| 4.2 | Pengujian dan Pembahasan | 48 |
| 4.2.1 | Pengujian FTP Server | 48 |
| 4.2.2 | Penerapan Keamanan SSL pada FTP Server | 51 |
| 4.2.3 | Pengujian dan Analisa FTP Server dengan SSL dan tanpa SSL..... | 53 |

BAB V PENUTUP

| | | |
|-----|------------------|----|
| 5.1 | Kesimpulan | 59 |
| 5.2 | Saran..... | 60 |

DAFTAR PUSTAKA

BIOGRAFI PENULIS

LAMPIRAN-LAMPIRAN

DAFTAR GAMBAR

| | Halaman |
|--|----------------|
| Gambar 2.1 Topologi Star..... | 9 |
| Gambar 2.2 Topologi Bus..... | 10 |
| Gambar 2.3 Topologi Ring | 11 |
| Gambar 3.1 Metode Waterfall..... | 26 |
| Gambar 3.2 Komponen Kerja FTP Client-Server..... | 28 |
| Gambar 3.3 Proses Kerja dari Secure Socket Layer (SSL)..... | 30 |
| Gambar 3.4 Proses uji FTP dengan SSL..... | 32 |
| Gambar 3.5 Topologi Serangan | 34 |
| Gambar 3.6 Flowchart Langkah Penerapan FTP Server..... | 37 |
| Gambar 3.7 Tampilan Pengalamatan Alamat IP..... | 39 |
| Gambar 3.8 Tampilan IP Forwarding | 39 |
| Gambar 3.9 Tampilan Firewall NAT Iptables | 40 |
| Gambar 3.10 Tampilan File Vsftpd.conf | 42 |
| Gambar 3.11 Tampilan Cara Kerja dari Algoritma Brute Force | 43 |
| Gambar 3.12 Tampilan Cara Kerja dari Xhydra Brute Force..... | 45 |
| Gambar 4.1 Tampilan Interface WinSCP | 48 |
| Gambar 4.2 Tampilan Proses Mengirim (Upload)..... | 49 |
| Gambar 4.3 Tampilan Hasil Proses Mengirim (Upload) Data..... | 49 |
| Gambar 4.4 Tampilan Proses Menerima (Download) data..... | 50 |
| Gambar 4.5 Tampilan Hasil Menerima (Download) data..... | 51 |
| Gambar 4.6 Tampilan Login dari FTP Client dalam Mode Enkripsi SSL. | 52 |
| Gambar 4.7 Tampilan dari Prosedur Handshake dengan Sertifikat..... | 53 |
| Gambar 4.8 Tampilan Tool Xhydra | 54 |
| Gambar 4.9 Tampilan Monitoring Serangan Xhydra FTP Server tanpa SSL | 55 |
| Gambar 4.10 Tampilan Monitoring Serangan Xhydra FTP Server Dengan SSL | 56 |
| Gambar 4.11 Tampilan Monitoring Serangan Xhydra dengan Fitur SSL . | 57 |

DAFTAR LAMPIRAN

| | Halaman |
|--|----------------|
| Lampiran 1. Lembar Pengajuan Judul | L-1 |
| Lampiran 2. Berita Acara Bimbingan Penulis Skripsi | L-2 |
| Lampiran 3. Hasil Plagiat <i>Checker</i> | L-5 |
| Lampiran 4. Surat Pemohonan Meja Hijau | L-6 |
| Lampiran 5. Kartu Bebas Praktikum..... | L-7 |

DAFTAR TABEL

| | Halaman |
|--|----------------|
| Tabel 2.1 Macam-Macam Layer TCP/IP | 12 |
| Tabel 2.2 Simbol Flowchart | 25 |
| Tabel 3.1 Daftar Alamat IP | 34 |
| Tabel 3.2 Biaya Keseluruhan | 36 |
| Tabel 4.1 Komponen Perangkat Keras..... | 46 |
| Tabel 4.2 Komponen Perangkat Lunak..... | 47 |

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan dunia teknologi komunikasi dan informasi semakin banyak perubahan untuk membantu manusia dalam mempermudah pekerjaan. Kebutuhan akan pertukaran data tidak hanya memanfaatkan media penyimpanan seperti DVD, CD, atau Flashdisk. Dengan jaringan yang ada di suatu lembaga pendidikan, pekerjaan dan di kehidupan sehari – hari itu sendiri sebagai media informasi dan komunikasi saat ini dirasa sangatlah perlu dimanfaatkan. Dengan memanfaatkan jaringan dalam melakukan pertukaran data dari komputer ke komputer lain melalui jaringan dapat disebut juga dengan *File Transfer Protocol* (FTP).

File Transfer Protocol (FTP) Server merupakan jenis sistem yang menghubungkan hak pengakses (*client*) dan penyedia (*server*) melakukan pertukaran data yang melewati port 21 (Ruwaida, Devi, Dian Kurnia, 2018). Sebenarnya *File Transfer Protocol* (FTP) tidak aman dalam melakukan pertukaran data atau file sebab data atau file dikirim tanpa melalui proses enkripsi terlebih dahulu tetapi melalui *clear text. Mode text* yang dipakai untuk pertukaran data adalah format ASCII atau format *binary*. Secara bawaannya (*default*), FTP menggunakan *mode ASCII* dalam pertukaran data. Karena dalam mengirim data tanpa enkripsi baik *username, password*, dan maupun perintah yang dikirim dapat di pantau oleh orang tidak bertanggung jawab. Solusi yang digunakan FTP *over*

SSL (FTPS) yang bekerja dengan data yang dikirim terlebih dahulu di enkripsi dengan adanya SSL pada FTP. *File Transfer Protocol* (FTP) server yang dilengkapi dengan *Secure Socket Layer* (SSL) diperlukan untuk menjaga proses autentikasi dan proses transfer data yang terlebih dahulu dienkripsi (Tehupeiory, Nardi *et al*, 2016).

Salah satu masalah yang belum diuji dan dianalisa untuk FTP server dengan keamanan SSL yaitu masalah dalam bocornya data login user dan admin pada FTP server oleh pihak yang tidak bertanggung jawab menjadikan data *password* FTP server bocor ketangan orang lain. Salah satu tindak kejahatan dalam jaringan yaitu penggunaan perangkat lunak Brute Force. Brute Force adalah salah satu teknik *hacking password* pada sebuah server, jaringan, atau *host*, dengan cara mencoba semua kemungkinan kombinasi *password* yang ada pada wordlist atau kamus *password*. Metode ini kemungkinan berhasil menemukan *password* yang ingin diretas.

Berdasarkan permasalahan tersebut penulis dapat membandingkan apakah FTP server akan aman bila menggunakan sertifikat SSL terhadap serangan Brute force dengan FTP server yang tidak menggunakan sertifikat SSL dan membuktikan apakah SSL mampu dalam mengamankan akun FTP server terhadap serangan Brute Force. Maka penulis mengadakan penelitian dalam bentuk tugas akhir yang berjudul **“ANALISIS KEAMANAN FTP SERVER DENGAN PROTOKOL SSL DARI SERANGAN BRUTE FORCE”**.

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka dapat di susun rumusan masalah sebagai berikut :

- a. Bagaimana membangun FTP server dengan *protocol* SSL pada jaringan *local*?
- b. Bagaimana membandingkan FTP server menggunakan keamanan *protocol* SSL dengan FTP server tanpa keamanan *protocol* SSL dari serangan Brute Force ?
- c. Bagaimana membuktikan FTP server yang dibangun dengan *protocol* SSL aman dari serangan Brute Force?

1.3 Batasan Masalah

Pada penelitian ini penulis membatasi ruang lingkup masalah agar peneliti lebih terarah pada objek yang dibahas, maka penulis membatasi masalah sebagai berikut :

- a. Menggunakan FTP server dengan *protcol* SSL pada jaringan *local*.
- b. Menggunakan jenis penyerangan Brute Force yang akan menyerang keamanan akun FTP server apakah FTP server dengan *protocol* SSL terhadap serangan Brute Force.
- c. Menggunakan aplikasi Vsftpd untuk FTP server dan menggunakan *Toolkit* atau openSSL.

1.4 Tujuan Penelitian

Dalam melaksanakan penelitian, penulis mempunyai tujuan yang akan dicapai. Adapun tujuan penelitian yang akan diperoleh penulis sebagai berikut :

- a. Dapat membangun FTP server dengan SSL pada jaringan local.
- b. Untuk mengetahui perbandingan antara FTP server yang menggunakan *protocol* SSL dengan FTP server yang tidak menggunakan *protocol* SSL.
- c. Untuk membuktikan FTP server yang dibangun dengan *protocol* SSL aman dari serangan Brute Force.

1.5 Manfaat Penelitian

Dalam penelitian ini diharapkan dapat memberikan manfaat yaitu :

- a. Penulis dapat membangun dan menganalisa FTP server dengan *protocol* SSL pada jaringan *local*
- b. Penulis Dapat mengetahui bahwa *protocol* SSL tidak hanya mengamankan dalam pertukaran data tetapi mampu atau tidaknya mengamankan data login akun user dan admin FTP server dengan *protocol* SSL.
- c. Penulis Dapat mengetahui perbandingan FTP server yang menggunakan SSL dengan FTP server yang tidak menggunakan *protocol* SSL dari serangan brute force.

BAB II

LANDASAN TEORI

2.1 Definisi Keamanan Jaringan

Keamanan jaringan adalah suatu proses perlindungan untuk mencegah dari berbagai ancaman terhadap serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab.

Keamanan jaringan komputer (*computer network security*) menjadi perhatian utama, ketika pada saat kita membangun sebuah infrastruktur jaringan. Kebanyakan arsitektur jaringan menggunakan router dengan *system firewall* yang terintegrasi (*built-in integrated firewall*), juga dukungan *software* jaringan yang dapat kemudahan akses kontrol, data *packet monitoring* dan penggunaan *protocol* yang diatur secara ketat (Sugiyono, 2016).

2.2 Jaringan Komputer

Jaringan komputer adalah "interkoneksi" antara 2 komputer *autonomous* atau lebih, yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). *Autonomous* adalah apabila sebuah komputer tidak melakukan kontrol terhadap komputer lain dengan akses penuh, sehingga dapat membuat komputer lain, *restart*, *shutdowns*, kehilangan file atau kerusakan sistem (Wongkar, stefen, Alicia Sinsuw, Xaverius Najoan, 2015).

Jaringan komputer merupakan adanya hubungan antar 2 atau lebih komputer melalui media lalulintas kabel atau tanpa kabel untuk saling

berkomunikasi dengan bertukar data. Dengan tujuan untuk salah satu komputer dapat melakukan permintaan dan pemberian layanan yang disebut dengan *Client-Server*.

Client-Server bekerja dengan *client* sebagai sistem dengan proses melakukan suatu permintaan (*Request*) layanan atau data pada *server* dimana *server* bekerja dengan melayani atau menyediakan data yang disediakan untuk *client*.

Terdapat beberapa jenis dari jaringan komputer yaitu:

a. *Local Area Network* (LAN)

Local Area Network (LAN) adalah jenis jaringan yang berukuran skala kecil seperti hubungan jaringan didalam wilayah sebuah kantor atau gedung. Jaringan LAN ini hanya dapat digunakan oleh pengguna yang ada pada dilingkungan area LAN saja.

LAN memiliki keuntungan dan kekurangan, untuk keuntungannya LAN iritnya dalam pengeluaran biaya operasional baik itu penggunaan kabel penerimaan data dan pengiriman dapat dilakukan dengan cepat dan lainnya. Kemudian dari sisi kekurangan LAN berada pada cakupan area dari koneksi LAN yang terbatas.

b. *Metropolitan Area Network* (MAN)

Metropolitan Area Network (MAN) adalah jenis jaringan yang mencakup sebuah wilayah atau kota, jaringan MAN dapat dikatakan gabungan dari beberapa jaringan LAN yang ada didalam satu wilayah.

MAN memiliki keuntungan dan kekurangan, dari segi keuntungan jaringan ini tentu lebih luas dari LAN yang dapat mencakup area yang lebih luas sehingga berkomunikasi dengan internet menjadi lebih efisien. MAN sendiri dapat mempermudah dalam halnya berbisnis. Bahkan, keamanan berkomunikasi menggunakan jaringan ini juga menjadi lebih terjaga. Untuk segi kekurangan MAN terdapat pada keamanannya meski telekomunikasi jaringan ini bisa dikatakan cukup aman, namun ternyata jaringan MAN mudah dirusak oleh pihak yang tidak bertanggung jawab untuk mengambil keuntungan pribadi atau yang lainnya dan untuk memperbaiki jaringan MAN ini memerlukan waktu yang cukup memakan waktu.

c. Wide Area Network (WAN)

Wide Area Network (WAN) adalah jenis jaringan yang mencakup area yang lebih luas, jaringan WAN biasanya digunakan untuk menghubungkan suatu jaringan dengan negara yang satu dengan lainnya dan dari suatu juga dapat daro benua satu ke yang lainnya. Untuk dapat menghubungkan ke hingga berbagai negara, jaringan WAN dapat terhubung dengan menggunakan kabel jenis *fiber optic* dan menempatkannya di dalam tanah maupun di jalur bawah laut.

2.3 Topologi Jaringan

Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Dalam suatu

jaringan komputer jenis topologi yang dipilih akan mempengaruhi kecepatan komunikasi (Halawa, 2016).

Topologi jaringan adalah suatu langkah yang dilakukan dengan menghubungkan beberapa komputer sehingga terbentuklah sebuah jaringan.

Ada beberapa topologi dengan jenis *Local Area Network* (LAN) yang sering digunakan yaitu:

a. Topologi *Star* (Bintang)

Topologi *Star* (Bintang) adalah topologi jaringan yang menggunakan hub/switch sebagai penghubung antar komputer dalam bertukar paket data. Topologi *Star* memiliki kontrol yang terpusat. Semua link harus melewati pusat yang menyalurkan data tersebut kesemua simpul atau client yang dipilihnya. Simpul pusat dinamakan stasiun primer atau server dan lainnya dinamakan stasiun sekunder atau client server. Setelah hubungan jaringan dimulai oleh server maka setiap client server sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari server.

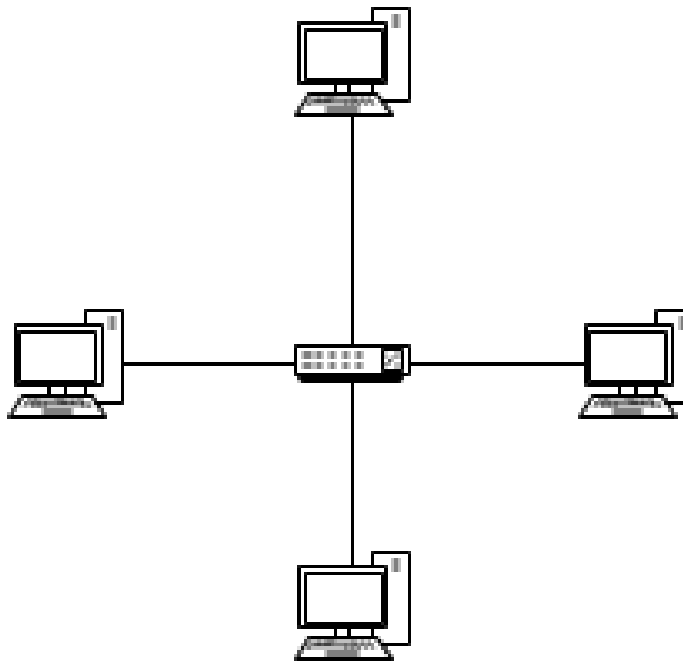
Kelebihan dari Topologi *Star* ini yaitu:

- 1) Kerusakan pada satu saluran hanya akan memengaruhi jaringan pada saluran tersebut dan station yang terpaut.
- 2) tingkat keamanan termasuk tinggi.
- 3) Tahan terhadap lalu lintas jaringan yang sibuk.
- 4) Kemudahan deteksi dan isolasi kesalahan/kerusakan pengelolaan jaringan.

Kelemahan dari Topologi *Star* ini yaitu:

- 1) HUB jadi elemen kritis karena kontrol terpusat.
- 2) Jaringan tergantung pada terminal pusat.
- 3) Biaya jaringan lebih mahal

Bentuk sederhana dari Topologi *Star* yaitu:



Gambar 2.1 Topologi *Star*

b. Topologi BUS

Topologi BUS adalah topologi jaringan komputer yang menggunakan sebuah kabel utama (*backbone*) sebagai tulang punggung jaringan.

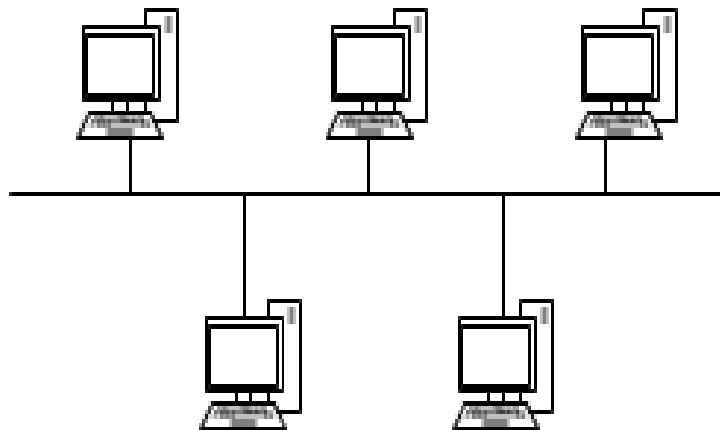
Keunggulan dari Topologi BUS ini yaitu:

- 1) Hemat kabel sehingga biaya instalasi relatif lebih murah.
- 2) Penambahan dan pengurangan terminal.

Kekurangan dari Topologi BUS ini yaitu:

- 1) Apabila terjadinya gangguan, maka akan sulit untuk mendeteksi kerusakan.
- 2) Sering terjadi kepadatan lalu lintas data pada jalur utama.
- 3) Apabila jalur utama mengalami kerusakan, seluruh jaringan akan lumpuh.
- 4) Memerlukan repeater untuk memperkuat sinyal.

Bentuk sederhana dari Topologi BUS yaitu:



Gambar 2.2 Topologi BUS

c. Topologi Ring (Token Ring)

Topologi Ring adalah topologi jaringan yang berupa ingkaran tertutup yang berisi node-node. Semua computer yang saling tersambung membentuk lingkaran (seperti Bus, tetapi ujungujungnya disambung). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebut sebagai loop. Data dikirimkan kesetiap simpul dan setiap informasi

yang diterima simpul diperiksa alamatnya apakah data itu untuknya atau bukan.

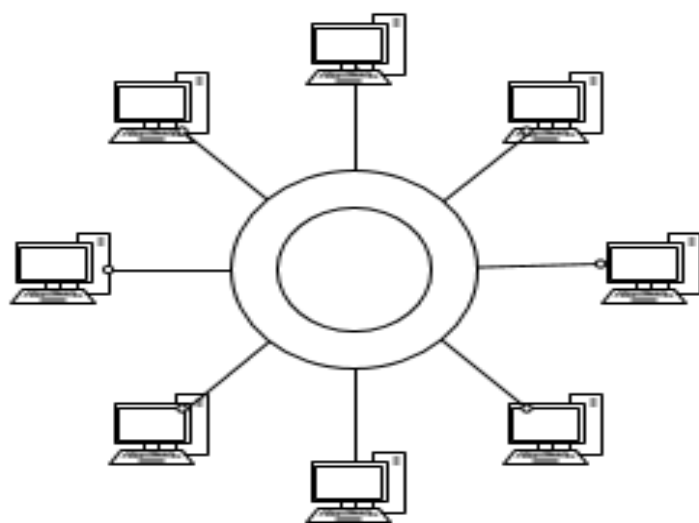
Keunggulan dari Topologi ini yaitu:

- 1) Dapat melayani aliran lalulintas data yang padat.
- 2) Aliran data mengalir lebih cepat karena dapat melayani data dari kiri atau kanan dari server.
- 3) Trasmisi data yang relatif sederhana seperti perjalanan paket data dalam satu arah saja.

Kelemahan dari topologi ini yaitu:

- 1) Kerusakan pada salah satu media pengirim/terminal dapat melumpuhkan kerja seluruh jaringan.
- 2) Paket data harus melewati setiap komputer antara pengirim dan penerima, sehingga menjadi lebih lambat.
- 3) Pengembangan jaringan menjadi lebih kaku karena penambahan terminal atau node menjadi lebih sulit bila port sudah habis.

Bentuk sederhana dari Topologi Ring yaitu:



Gambar 2.3 Topologi Ring

2.4 *Transmission Control Protocol/Internet Protocol (TCP/IP)*

Transmission Control Protocol/Internet Protocol (TCP/IP) adalah protokol yang paling sering dan banyak digunakan dalam standar untuk melakukan komunikasi data dikarenakan memiliki banyaknya kelebihan. *Transmission Control Protocol/Internet Protocol (TCP/IP)* merupakan sebuah standar jaringan terbuka yang memiliki sifat independen terhadap mekanisme *transport* jaringan fisik yang digunakan, sehingga dapat digunakan dimana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut dengan *IP Address* (Alamat IP) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling terhubung satu sama lainnya (Syarifuddin, M, Beni Andika, Rico Imanta Ginting, 2017).

Terdapat 5 *layer* (lapis) yang ada pada TCP/IP dapat dijelaskan dalam bentuk tabel berikut:

Tabel 2.1 Macam-macam Layer TCP/IP

| NO | Layer | Keterangan |
|----|-----------------------|---|
| 1 | <i>Physical Layer</i> | <i>Physical Layer</i> dapat diartikan dengan karakteristik dimana hardware membutuhkannya dalam membawa sinyal data transmisi. Contoh dari hardware ini yaitu kabel dikarenakan cara kerja pada layer ini menerjemahkan sinyal listrik menjadi data digital yang dipahami komputer. |

| | | |
|---|------------------------|--|
| 2 | <i>Internet Layer</i> | <i>Internet Layer</i> bekerja dalam proses pengiriman data yang dikirim hingga sampai ke alamat yang diterima dengan tepat contoh protokol dari <i>layer</i> ini seperti <i>Internet Protocol</i> (IP) protokol yang mengurus alamat untuk mengirim dan menerima data hingga sampai tujuannya. |
| 3 | <i>Trasnport Layer</i> | <i>Trasnport Layer</i> bekerja sebagai <i>layer</i> yang mengatur komunikasi data yang saling terhubung dalam keperluan aplikasi <i>layer</i> dan internet layer. Contoh <i>host</i> dari <i>Trasnport Layer</i> yaitu <i>Transmission Control Protocol</i> (TCP) dan <i>User Datagram Protocol</i> (UDP). |
| 4 | Application Layer | Application Layer bekerja dengan menyediakan semua aplikasi yang menggunakan protokol TCP/IP yang nantinya dapat berhubungan langsung dengan user. Contohnya seperti penggunaan layanan TELNET,SMTP, FTP, dan yang lainnya. |

2.5 FTP Server dan FTP Client

FTP server adalah suatu server yang menjalankan software yang berfungsi untuk memberikan layanan tukar menukar data atau file dimana sever tersebut selalu siap memberikan layanan FTP apabila mendapat permintaan (request) dari FTP client (Nurdin, 2008)..

FTP Server adalah komputer yang bekerja dengan menyediakan data *storage* untuk client dalam menyimpan, mengirim, mengambil data yang ada didalam server atau yang telah diolah oleh client.

FTP client adalah komputer yang merequest koneksi ke FTP server untuk tujuan tukar menukar file. Setelah terhubung dengan FTP server, maka client dapat men-download, meng-upload, merename, men-delete, dll sesuai dengan permission yang diberikan oleh FTP server.

File Transfer Protocol (FTP) berjalan dengan memanfaatkan layanan protokol TCP layer (lapisan) 4 dalam melakukan operasinya, kemudian dalam proses kerja FTP bekerja dengan memanfaatkan port 21 dan 20.

2.6 Protokol SSL

Secure Socket Layer adalah protokol khusus atau jalur khusus yang lebih aman pada website dimana semua transaksi data yang menggunakan protokol tersebut akan di enkripsi (Rosmala, 2013). Teknologi SSL menggunakan konsep teknologi kriptografi kunci publik untuk bisa mencapai komunikasi yang aman ini antara server dan pengunjungnya. Kedua pihak yang berkomunikasi ini (server dan pengunjungnya) saling mengirimkan data yang disamarkan dan untuk membacanya digunakan sandi dan kunci yang hanya dimiliki kedua pihak yang berkomunikasi tersebut, sehingga pihak lain yang mencoba menyadap data yang dikirim tersebut tidak akan bisa membacanya karena sandi dan kunci yang dibutuhkan tersebut hanya dimiliki oleh kedua pihak yang berkomunikasi dengan menggunakan SSL untuk mengamankan transmisi data melalui internet dengan

cara *enkripsi*, sehingga hanya penerima pesan yang dapat memahami hasil dari data yang sudah dienkripsi tersebut. Pada saat sertifikat ssl digunakan pesan tidak dapat terbaca oleh siapapun kecuali ke server yang memang dituju saat mengirim pesan tersebut. Sehingga data atau informasi terlindungi dari *hackers* dan pencuri identitas. Kegunaan utamanya adalah untuk menjaga keamanan dan kerahasiaan data ketika melakukan transaksi.

2.7 Brute Force Attack

Brute Force Attack adalah metode untuk meretas *password* (*password cracking*) dengan cara mencoba semua kemungkinan kombinasi yang ada pada "*wordlist*". Metode ini dijamin akan berhasil menemukan *password* yang ingin diretas. Namun, proses untuk meretas *password* dengan menggunakan metode ini akan memakan banyak waktu. Lamanya waktu akan ditentukan oleh panjang dan kombinasi karakter *password* yang akan diretas (Sanjaya, Romy, Ardika, 2014).

Brute Force Attack adalah metode mengalahkan skema kriptografi dengan mencoba semua kemungkinan *password* atau kunci. Brute force attack memungkinkan bisa menyerang kunci privat di hampir semua skema kriptografi, tipe serangan ini bergantung pada ukuran kunci dan mekanisme pada enkripsi yang digunakan (Wicaksono, Lutfi, 2016). Semakin besar ukuran kunci dari kunci privat akan semakin sulit dibobol oleh brute force attack, kriptografi kunci publik sangat ditentukan oleh kuncinya. Semakin sulit pemecahan algoritma kuncinya maka tingkat keamanannya semakin tinggi.

2.8 Linux

Linux adalah salah satu OS yang menganut sistem UNIX dan menggunakan model pengembangan dan distribusi software secara gratis, atau biasa dikenal dengan istilah open source. Seperti halnya aplikasi open-source lainnya, Linux juga bisa dikembangkan dan didistribusikan secara gratis, inilah yang menjadi salah satu daya tarik dari OS ini.

Yang dimaksud Linux adalah perangkat lunak atau software sistem operasi yang sifatnya open source dan gratis untuk di dapatkan maupun di sebarluaskan dengan lisensi GNU. OS Linux merupakan turunan dari unix dan dapat digunakan pada bermacam-macam komputer. Dengan Linux maka pengguna dapat memperoleh software yang lengkap dengan source code-nya. Bahkan pengguna dapat mengubah atau memodifikasi source code-nya, dan semua itu legal tentunya di bawah lisensi GNU. Pada os Linux ini kebebasan dan gratis lah yang paling utama, sehingga pengguna mendapatkan source code-nya dan tentunya hal ini sangat menguntungkan bagi para programmer maupun para administrator. Sedangkan nama Linux diambil dari nama yang membuatnya ialah Linus Torvalds, Linux diperkenalkan pada tahun 1991. Saat ini OS Linux sudah banyak digunakan di Indonesia karena memiliki banyak keunggulan terutama untuk sistem operasi server karena sifatnya yang gratis dan sangat handal. Linux sendiri saat ini terus berkembang, beberapa sistem operasi linux yang populer misalnya seperti Ubuntu, Fedora, Debian, dan sebagainya.

Linux sebagai sistem operasi tentu memiliki kelebihan dan kekurangan, untuk kelebihan dari sistem operasi linux yaitu:

- a. Linux dapat diperoleh secara bebas tanpa perlu adanya membeli lisensi. Pengguna linux juga dapat melakukan download kode sumber dari linux bila ingin melihat tanpa dibatasi apapun.
- b. Linux mengoleksi *software* tersendiri yang cukup begitu lengkap untuk keperluan desktopnya baik laptop dan PC server. Bila *software* yang disediakan terasa adanya kekurangan maka pengguna dapat menambahkan dengan mudah melalui repository yang tersedia dan disediakan.
- c. Dalam pengoperasiannya linux sangat stabil dikarenakan jarang sekali linux mengalami crash atau hang. Pengguna tidak perlu lagi dan tidak pernah melakukan restart apabila melakukan konfigurasi terhadap sistem.
- d. Linux jarang terkena virus dikarenakan selain jumlah virus yang ada di linux sedikit, Linux pula sangat ketat dalam hal mengelola keamanan.
- e. Dikarena linux dikembangkan secara komunitas dan setiap komunitas dapat memberikan masukan-masukan dan perbaikan untuk bug atau cacat tersebut Dengan menggunakan sistem operasi linux terutama pada perbaikan bug atau cacat yang ada pada linux begitu cepat terselesaikan.

Kemudian untuk kelemahan dari sistem operasi linux itu sendiri yaitu:

- a. Sistem operasi linux kurang memiliki dukungan dari produsen perangkat keras dengan begitu penyediaan *software driver*. Hampir semua *software driver* yang saat ini ada di linux merupakan hasil dari

usaha komunitas linux, dan sebagian kecil murni dukungan dari produsen perangkat keras.

- b. Sistem operasi linux kurang didukung oleh beberapa pengembang software terutama pada game. Kebanyakan developer game masih mengarah pada sistem operasi Microsoft Windows sebagai platform gamenya.

2.9 Wireshark

Wireshark merupakan sebuah *tools* yang dipergunakan untuk memonitoring trafik data jaringan dengan manfaat agar pengguna dapat mengetahui apakah trafik data jaringan dalam keadaan normal atau mengalami masalah pada lalu lintas data didalam jaringan itu sendiri.

Software wireshark network protocol analyzer bekerja dengan menangkap semua trafik selama menggunakan jaringan *internet*, baik *ip address*, *protocol*, lalu informasi didalam paket data itu sendiri dengan tujuan user atau pengguna dalam menggunakan *wireshark* adalah untuk memudahkan dalam melihat dan menganalisa paket data dalam lalu lintas jaringan internet (Sihombing, Rolan, Muhammad Zulfi, 2013).

Terdapat beberapa kelebihan dari wireshark yaitu:

- a. Multiplatform – wireshark dapat dioperasikan pada beberapa platform sistem operasi seperti Mac, Windows, Linux, dan Unix.
- b. Wireshark mudah didapatkan dan juga *Open Source* (Gratis)

- c. Wireshark mampu melakukan *capture paket* (menangkap) data jaringan secara *real time*.
- d. Wireshark mampu menampilkan informasi protokol jaringan dari paket data secara lengkap.
- e. Wireshark menghasilkan Paket data yang dapat disimpan menjadi sebuah file dan nantinya dapat dibuka kembali untuk dianalisis.
- f. Wireshark mencari paket data dengan kriteria spesifik.
- g. Wireshark memberikan fitur pewarnaan antarmuka paket data untuk memudahkan dalam analisa paket data.

2.10 Sistem Operasi Ubuntu

Ubuntu dirilis untuk pertama kali pada tahun 2004, Ubuntu adalah sebuah Sistem Operasi, Ubuntu ini biasanya lebih dikaitkan untuk membangun sebuah server. Yang Berfungsi sebagai:

- a. Penyedia Layanan (Seperti DNS server, Mail Server, Proxy Server, Dan Lainnya),
- b. Pengatur Proses Jaringan (Seperti Fungsi Router, Repeater, Dan Lainnya)
- c. Berfungsi untuk melakukan troubleshooting, dalam artian bisa mendeteksi kesalahan yang ada pada *hardware, software*, maupun *network* (jaringan)

Mengapa menggunakan sistem operasi ubuntu:

- a. *Open source* dan gratis

Salah satu alasan mengapa sistem operasi Ubuntu begitu populer yaitu dikarenakan ubuntu mudah didapatkan dengan gratis dan *open source*. pengguna tidak perlu mengeluarkan dana untuk mendownload, menginstall, dan menggunakan Ubuntu. pengguna hanya perlu mendownload melalui website resmi dari ubuntu itu sendiri. Kemudian selain dari itu *software-software* yang tersediapun gratis. Ubuntu dikatakan *open source* dikarenakan pengguna dapat menemukan *source code* dengan mudah diluar sana untuk Ubuntu. Ini pula yang mengarahkan bahwa siapa saja bisa melakukan modifikasi yang lebih baik untuk sebuah perangkat lunak.

b. Penggunaan yang mudah

Kebanyakan pengguna komputer berfikir bahwa sistem operasi dengan berbasis Linux sulit untuk dioperasikan dan lebih dominan digunakan oleh seorang pengembang. Namun ubuntu Linux adalah sistem operasi berbasis Linux yang masih tergolong mudah digunakan dan *user friendly*. Siapa saja dapat mengoperasikan Ubuntu dan semua orang dengan memiliki kemampuan dibidang komputer atau tidak dapat melakukan pengaturan sistem. perusahaan *Canonical* terus mengembangkan Ubuntu agar memberikan antarmuka yang mudah dinavigasi dan meningkatkan *user experience*.

c. Aman dalam penggunaan

Ubuntu dapat dikatakan sebagai salah satu sistem operasi yang aman. Dengan built in *Firewall* dan proteksi virus yang kuat ini tentu pengguna tidak perlu lagi memasang sebuah anti *virus* didalamnya.

d. Kuatnya *support*

Ada banyak *support* komunitas yang bisa pengguna manfaatkan bila pengguna memiliki pertanyaan-pertanyaan mengenai Ubuntu. Untuk mendapatkan *support* gratis, pengguna dapat mengunjungi As Ubuntu, *LinuxQuestions*, dan *website* resmi Linux.

e. Mudah dimodifikasi

Ubuntu sangat mudah dimodifikasi. Ada banyak lingkungan *desktop* alternatif yang dapat pengguna gunakan. pengguna bahkan dapat mengatur agar Ubuntu pengguna memiliki tampilan seperti Windows atau sistem operasi lain yang diinginkan.

f. Dapat melakukan banyak hal dengan Ubuntu

Dengan sistem operasi ubuntu, pengguna dapat melakukan banyak hal dari mengedit dokumen, bekerja dengan foto dan video, dan masih banyak lagi.

2.11 Virtual Box

Oracle VM Virtual Box adalah salah satu aplikasi virtualisasi (*Hypervisor*), dimana dapat di-*install* pada komputer baik *physical*, baik yang berbasis intel maupun AMD, tidak membutuhkan fitur processor yang dibangun dalam hardware baru seperti intel Vt-x atau AMD-v. Bahkan Oracle VM Virtual

Box dapat digunakan pada *hardware/processor* lama yang tidak mendukung *hardware virtualization* (Larosa, 2016).

VirtualBox adalah perangkat lunak untuk memvirtualisasikan pengguna dalam instalasi dan menggunakan sistem operasi didalam sistem operasi atau dapat digunakan untuk menjalankan sistem operasi lain di dalam sistem operasi utama. Contoh, bila pengguna memiliki sistem operasi Windows 7 yang menjadi sistem operasi inti di komputernya, maka pengguna tersebut ingin merasakan sistem operasi lain dapat dijalankan sesuai yang diinginkan di dalam sistem operasi intinya tersebut menggunakan VirtualBox.

Manfaat Menggunakan Virtualbox :

- a. Bermanfaat bagi pemula dalam belajar menginstall operasi sistem, tanpa perlu adanya ubahan data data yang ada di hardisk.
- b. Bermanfaat dalam menginstall beberapa operasi sistem secara bebas tanpa harus mengawatirkan bahwa sistem operasi tersebut tersimpan secara permanent di dalam hardisk, dimana fungsi ini penting untuk pengguna yang hendak ingin melakukan ujicoba dan simulasi instalasi suatu sistem tanpa harus kehilangan sistem yang ada.

Mengenal fitur network adapter pada virtualbox:

Dalam bentuk perangkat kerasnya network adapter merupakan bagian dari perangkat keras langsung yang digunakan untuk menghubungkan komputer dengan jaringan, akan tetapi pada virtualbox *network* adapter di virtualisasikan sehingga tidak berhubungan langsung dari perangkat kerasnya langsung, didalam virtualbox penggunaanya disediakan dengan 4

adapter dengan cara mengaktifkannya begitu cukup mudah hanya dengan centang salah satu adapter tersebut. Berikut tipe dari adapter yang tersedia pada virtualbox:

a. *Not Attached*

Ketika pengguna memilih tipe ini maka pengguna berarti tidak menggunakan jenis network adapter apapun yang mana ini berarti jaringan yang terhubung pada virtualbpx nantinya tidak ada.

b. *Network Address Translation (NAT)*

Tipe adapter ini bekerja dengan menggunakan satu ip saja dari Perangkat keras utama. Pada adapter jenis ini pengguna menggunakannya untuk menjalin koneksi dengan internet dan tidak cocok sebagai jaringan komputer langsung terhubung pada komputer lain di karenakan komputer lain tidak akan mengenali alamat ip dari guest virtualbox.

c. *Bridge Adapter*

Tipe adapter ini bekerja dengan menggabungkan dua *interface* yang berbeda atau menjembatani antara adapater komputer utama dengan adapter untuk virtualbox. Yang dijembatani disini adalah adapter perangkat keras dan adapter virtual. Adapter ini akan menjadikan adapter perangkat keras dan virtual menjadi satu jaringan. contohnya adapter perangkat keras beralamatkan ip 192.168.43.5/24, maka yang akan terjadi adalah adapter virtual akan mengikuti urutan alamat ip pada adapter perangkat keras yaitu 192.168.43.xxx/24 . Adapter jenis

ini akan berguna jika ingin menghubungkan komputer fisik dengan komputer di virtualbox, maupun menghubungkan komputer virtualbox di hubungkan dengan komputer lain dalam jaringan atau pun dengan internet. Adapter ini bisa memilih perangkat keras mana yang akan digunakan.

d. *Internal Network*

Type adapter ini bekerja dengan menghubungkan 2 atau lebih sistem operasi virtual yang telah terinstall menjadi satu jaringan dan komputer utama tidak bisa bergabung kedalam jaringan yang sama dengan jaringan virtual. Secara nyata, fungsi adapter ini layaknya sebuah *hub/switch*.

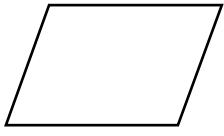
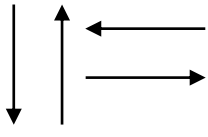
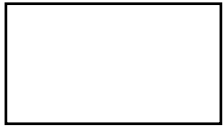
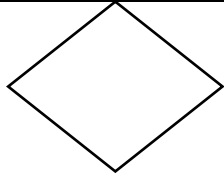
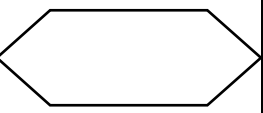
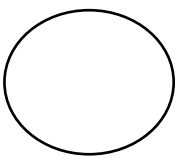

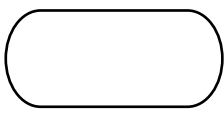
e. *Host Only Adapter*

Type adapter ini bekerja seperti layaknya tipe adapter *internal network*, perbedaan dengan adapter ini dengan *internal network* yaitu komputer utama dapat berhubungan dengan sistem operasi virtual. Kelebihan lainnya, adapter ini bisa digandakan sesuai kebutuhan, kemudian pada adapter ini virtualbox menyediakan drivernya sendiri khusus untuk adapter ini.

2.12 Flowchart

Flowchart adalah adalah suatu bagan dengan simbol-simbol tertentu yang menggambarkan urutan proses secara mendetail dan hubungan antara suatu proses (instruksi) dengan proses lainnya dalam suatu program.

Tabel 1. Simbol Flowchart

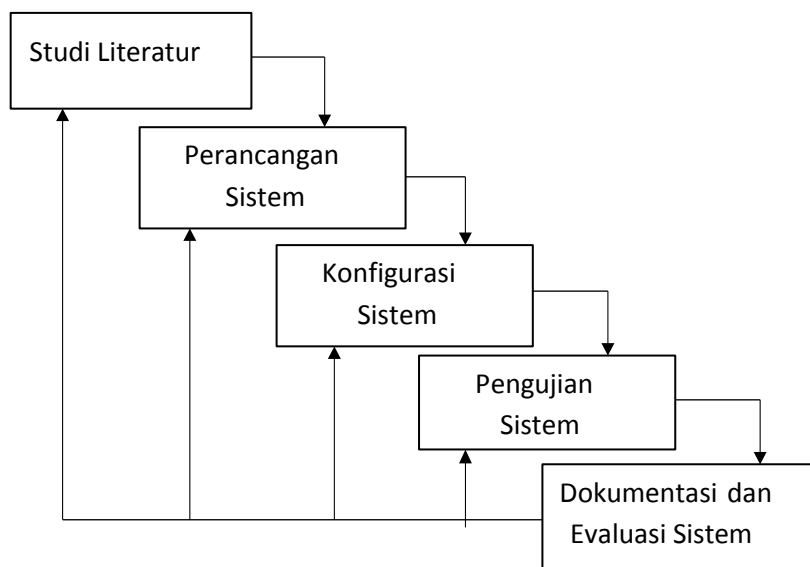
| Simbol | Keterangan |
|---|--|
|  | <p>Input/Output</p> <p>Digunakan untuk mewakili data input/output</p> |
|  | <p>Arus/Flow</p> <p>Digunkana untuk menunjukkan arah/alir dari suatu proses.</p> |
|  | <p>Proses</p> <p>Digunakan untuk mewakili suatu proses.</p> |
|  | <p>Keputusan/<i>Decision</i></p> <p>Digunakan untuk suatu penyelesaian kondisi dalam program.</p> |
|  | <p>Persiapan/ <i>pendefined</i> Proses</p> <p>Digunakan untuk memberikan nilai awal dari proses.</p> |
|  | <p>Penghubung/<i>Connector</i></p> <p>Digunakan untuk menunjukkan sambungan dari aliran yang terputus dihalaman yang sama.</p> |
|  | <p><i>Predefined</i> proses</p> <p>Digunakan untuk proses yang detilnya terpisah.</p> |
|  | <p>Awal/akhir (Terminal)</p> <p>Digunakan untuk menunjukkan awal dan akhir dari proses.</p> |

BAB III

METODE PENELITIAN

3.1 Tahap Penelitian

Metode yang digunakan dalam membangun penelitian ini adalah metode *waterfall*, metode ini mengarah pada pengumpulan data, , karena dengan mendapatkan data yang tepat maka penelitian akan berlangsung sesuai dengan rumusan masalah yang telah ditentukan, seperti berikut:



Gambar 3.1 Metode *waterfall*

3.2 Metode Pengumpulan Data

a. Studi Literatur

Dengan pengumpulan data-data berupa teori baik dengan dosen pembimbing maupun dengan orang yang berkompeten dalam kasus ini dan pustaka yang mendukung.

b. Perancangan Sistem

Meliputi beberapa tahap yang terstruktur sebagai berikut :

a. Sistem dirancang menggunakan sistem operasi dan konfigurasi linux, paket pendukung linux dan Vsftpd, menggunakan sistem operasi windows sebagai pengujian.

b. Hasil dan pembahasan dengan cara menguji dan menganalisa FTP Server dengan keamanan.

c. Konfigurasi Sistem

Dalam skripsi ini sistem yang dikonfigurasi yaitu menggunakan linux debian, Vsftpd, dan juga Openssl sebagai sistem yang nantinya sebagai FTP Server dengan SSL.

d. Pengujian Sistem,

Melakukan analisa dalam pengujian dan penaksiran ulang sistem yang telah melakukan konfigurasi.

e. Dokumentasi dan Evaluasi Sistem

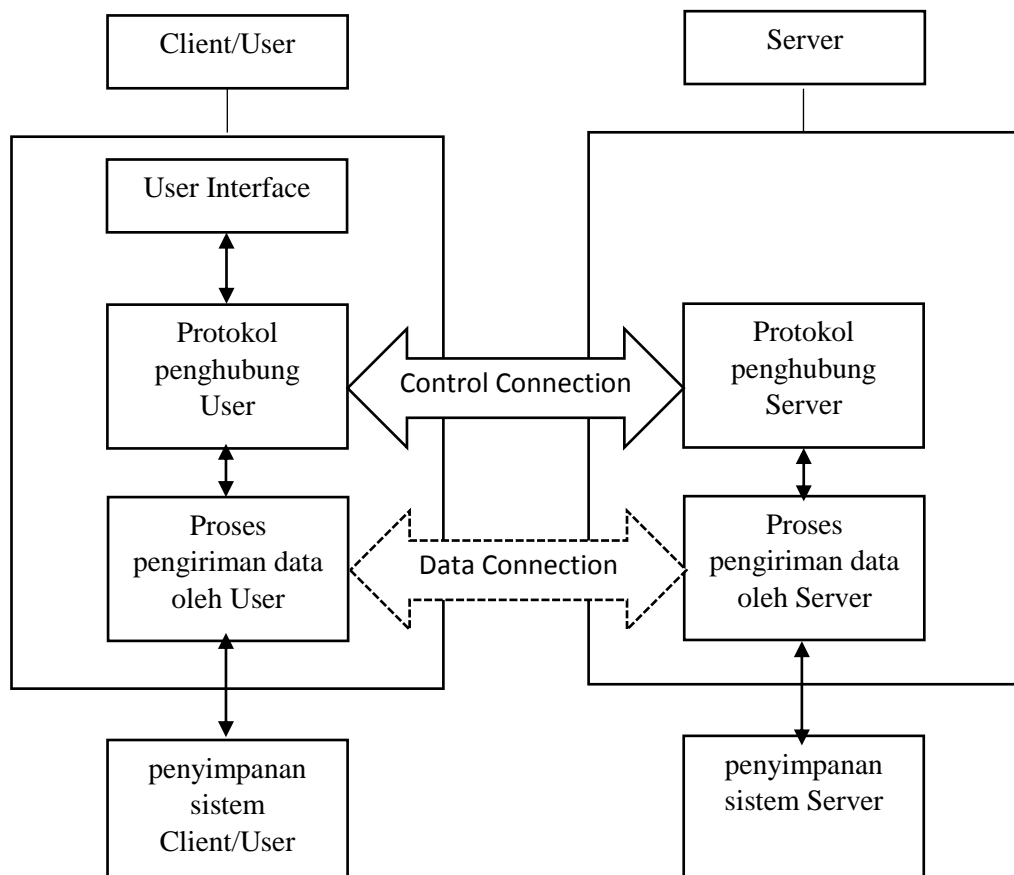
Apakah sistem yang telah di miliki mendapatkan hasil yang baik dan analisa dengan tingkat yang baik untuk dilakukan analisa lebih lanjut.

3.3 Analisis Sistem Sedang Berjalan

Terdapat alur dalam proses kerja dari *File Transfer Protocol* (FTP) yaitu mengirim (*Upload*) dimana proses ini dilakukan dengan mengirim data dari user atau komputer client kepada penyedia FTP server adalah komputer server dan proses meminta (*Download*) dapat dilakukan dengan user atau komputer client

melakukan pengambilan atau meminta data yang disediakan oleh komputer server. *File Transfer Protocol* (FTP) server membutuhkan *Secure Socket Layer* (SSL) untuk mengamankan dalam komunikasi pertukaran data sebab FTP yang digunakan tanpa adanya SSL beresiko tidak aman, FTP bekerja dengan *transparent* dalam melakukan pertukaran data tanpa adanya proses enkripsi didalamnya. Sehingga akan beresiko terjadinya penyerangan yang merugikan pihak penyedia FTP server itu sendiri.

Komponen kerja dari File Transfer Protocol (FTP) Client-Server tanpa adanya keamanan SSL. Seperti berikut:



Gambar 3.2 Komponen Kerja FTP Client-Server

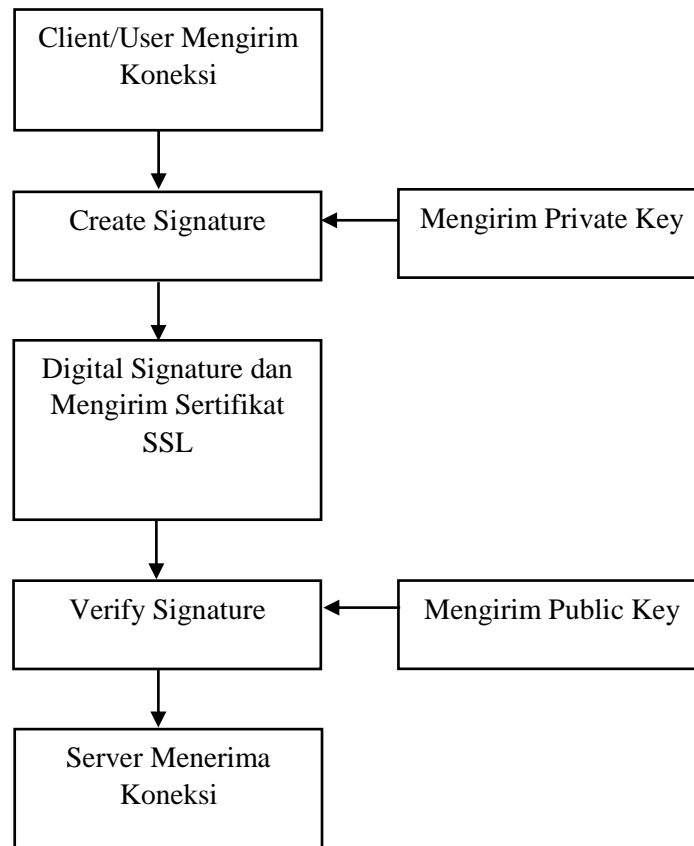
Dalam gambar 3.2 dapat dijelaskan bahwa *File Transfer Protocol* (FTP) menggunakan *protocol* TCP dengan 2 komunikasi dalam proses kerjanya yaitu Client dan Server. Untuk menghubungkan Client dengan Server terdapat 2 jembatan komunikasi yaitu *Control Connection* dan *Data Connection*.

- a. *Control Connection* bekerja pada saat Client melakukan sesi pertukaran informasi atau komunikasi data Antara Client dan Server.
- b. *Data Connection* bekerja saat data (file) yang diminta oleh Client pada Server baik sebaliknya dan *Data Connection* akan berhenti ketika file yang diminta sampai pada Client. Proses *Data Connection* akan dihentikan.

Dari 2 jembatan komunikasi yang telah ada untuk membedakan kedua jembatan tersebut digunakan komponen proses dari FTP itu sendiri yaitu *Protocol Interpreter* dan *Data Transfer Process*.

- a. *Protocol Interpreter* bekerja dengan mengatur koneksi yang berhubungan dengan penerimaan dan pengiriman perintah koneksi.
- b. *Data Transfer Process* bekerja dengan mengatur hal yang berhubungan dengan pertukaran data (file).

Protocol Secure Socket Layer (SSL) dipergunakan pada FTP untuk mengamankan proses pertukaran data FTP. proses kerja dari *Secure Socket Layer* (SSL) sebagai berikut:



Gambar 3.3 Proses kerja dari Secure Socket Layer (SSL)

Melalui gambar 3.3 dapat dijelaskan bahwa SSL memungkinkan Client dan Server berkomunikasi pada jaringan yang aman dari pihak luar. Dengan memanfaatkan dua buah kunci, yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk enkripsi data, sedangkan kunci privat digunakan untuk dekripsi data. Data diubah menjadi hash. Fungsi hash mengubah masukan menjadi sebuah beberapa karakter yang panjangnya tetap dan tertentu yang disebut inti dari data. Kemudian, inti data di-enkripsi oleh kunci *privat* menjadi *Digital Signature*. Untuk membuka tanda tangan digital tersebut diperlukan kunci publik. Bila data telah diubah oleh pihak luar, maka tanda tangan digital juga ikut berubah sehingga kunci publik yang ada tidak akan bisa membukanya. Ini merupakan salah satu

syarat keamanan jaringan, yaitu *Authenticity*. Artinya adalah, keaslian data dapat terjamin dari perubahan-perubahan yang dilakukan pihak luar. Dengan cara yang sama, pengirim data tidak dapat menyangkal data yang telah dikirimkannya. Bila tanda tangan digital cocok dengan kunci privat yang dipegang oleh penerima data, maka dapat dipastikan bahwa pengirim adalah pemegang kunci privat yang sama. Ini berarti Digital Signature memenuhi salah satu syarat keamanan jaringan, yaitu Nonrepudiation atau non-penyangkalan.

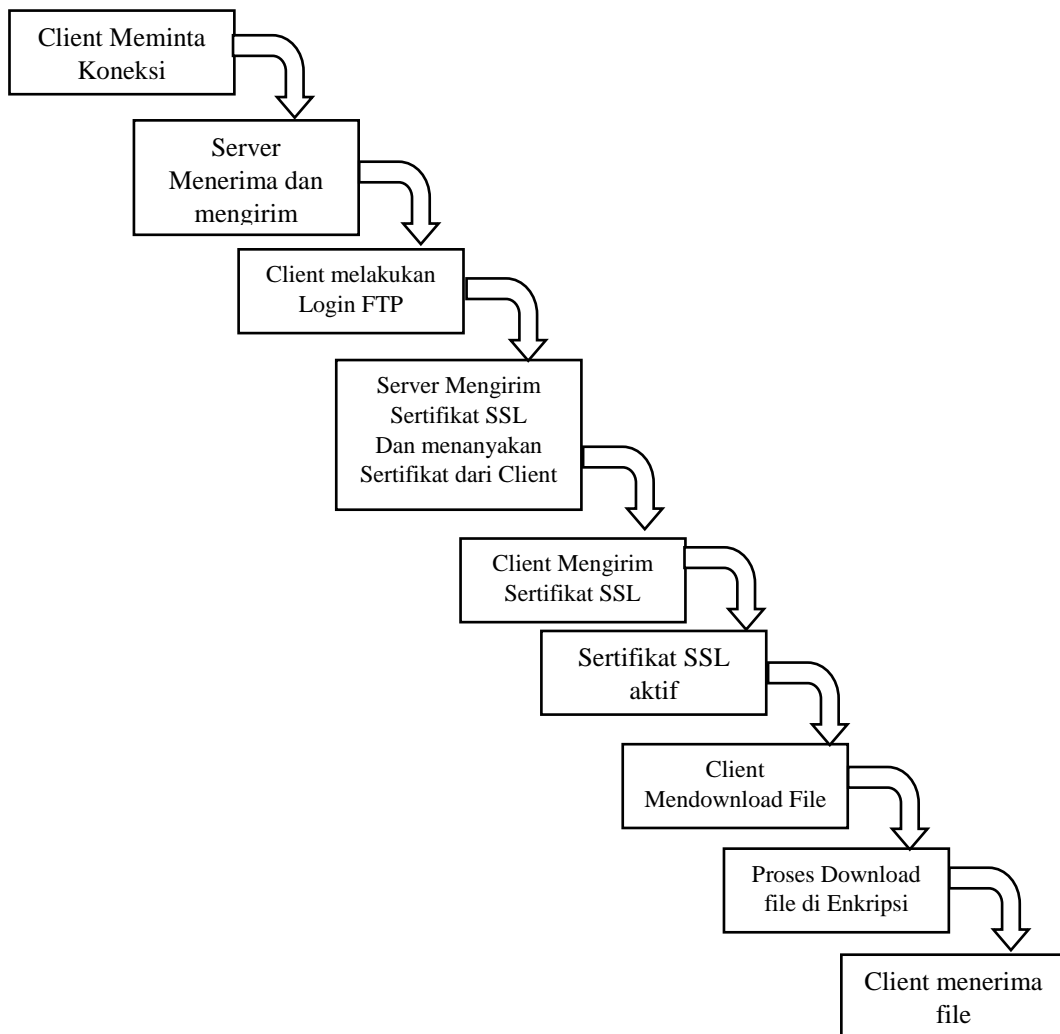
Sebuah FTP Server dengan SSL, Client dan server menegosiasikan sebuah koneksi dengan menggunakan sebuah prosedur *handshaking* (jabat tangan). Selama handshake ini, klien dan server menyetujui berbagai parameter digunakan untuk menetapkan keamanan koneksi.

- a. *Handshaking* dimulai ketika sebuah klien mengkoneksi ke sebuah server dengan SSL aktif atau-enable yang membutuhkan sebuah koneksi yang *secure* dan menampilkan daftar CipherSuites (*ciphers* dan *hash functions*) yang didukung.
- b. Dari daftar tersebut, server memilih salah satu cipher dan hash function yang paling kuat dan menotifikasi klien untuk pengambilan keputusan.
- c. Server mengirim balik identifikasinya dalam bentuk sebuah sertifikat digital. Atau yang lebih dikenal sebagai *Certificate Signing Request* (CSR). Sertifikat ini biasanya mengandung nama server, *certificate authority* (CA), dan *public encryption key* dari server.
- d. Klien kemudian akan menghubungi server bahwa sertifikat digital tersebut benar valid sebelum memulai proses.

e. Dalam rangka menghasilkan *session keys* yang digunakan untuk *secure connection*, klien mengenkripsi sebuah nomor acak dengan mengirim hasilnya ke server. Hanya server yang bisa mendekripsinya dengan *private key* server.

f. Dari nomor acak, kedua belah pihak menghasilkan material *key* untuk enkripsi dan dekripsi.

Cara kerja dari *File Transfer Protocol* (FTP) Server dengan keamanan SSL dapat dideskripsikan langkah pengujian yang dilakukan penulis sebagai berikut:



Gambar 3.4 Proses uji FTP dengan SSL

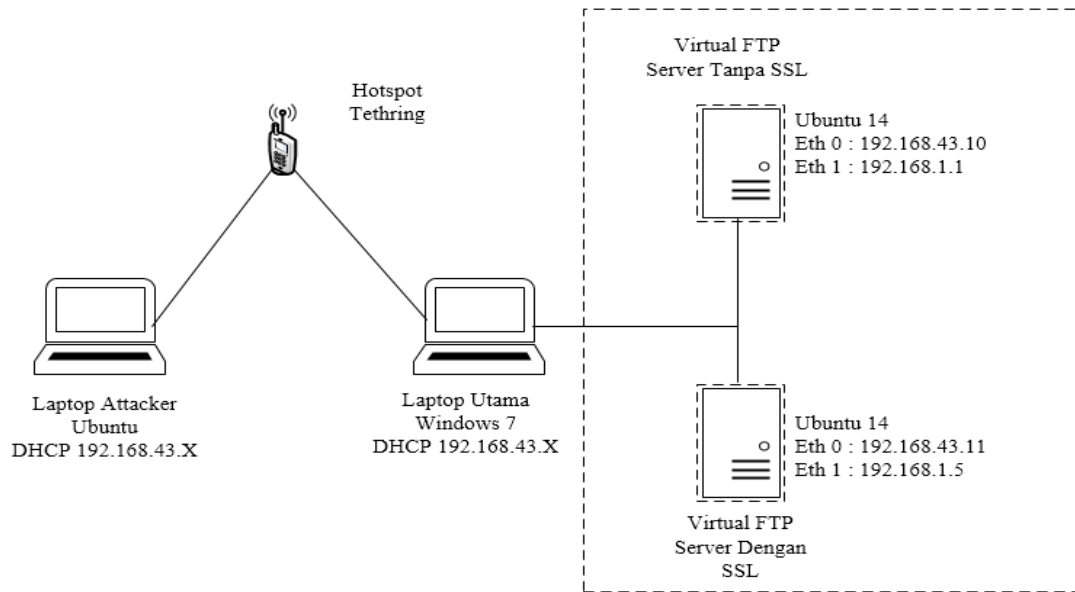
Pada gambar 3.4 menjelaskan proses Client melakukan permintaan koneksi pada server dan koneksi Client diterima oleh Server kemudian dikembalikan kepada Client dengan tambahan Server mengajukan Sertifikat SSL sebagaimana untuk memastikan koneksi dari client dilakukan hanya Client dengan Server

3.4 Rancangan Penelitian

Dalam tugas akhir ini nantinya akan dibangun FTP Server dengan *Protocol* SSL, menerapkan sebuah serangan terhadap FTP Server dengan SSL dan tanpa SSL menggunakan serangan Brute Force. Menganalisa apakah protocol SSL dapat mengamankan FTP dari serangan Brute Force.

Dalam membangun FTP Server itu sendiri peneliti menggunakan *tools* Virtualbox, Virtualbox itu sendiri merupakan perangkat lunak yang memungkinkan pengguna dalam melakukan instalasi sistem operasi secara virtualisasi. Dengan begitu pengguna dapat bereksplorasi baik itu dalam instalasi atau yang lainnya. Dalam penelitian ini penulis membangun 2 FTP Server dengan yang satunya terdapat keamanan SSL kemudian ada pula 1 Client yang nantinya bekerja sebagai *attacker*.

Sistem yang akan dibangun dapat digambarkan dengan topologi serangan berikut:



Gambar 3.5 Topologi Serangan

Dalam gambar 3.5 Diatas dapat dijelaskan dengan pengalamatan IP pada tabel berikut ini:

Tabel 3.1 Daftar Alamat IP

| NO | Perangkat | Port Ethernet | Alamat IP / IP Address |
|----|--------------|---------------|---|
| 1 | Laptop Utama | Wifi | Address DHCP 192.168.43.X Netmask 255.255.255.0 Gateway 192.168.43.1 |

| | | | |
|---|----------------------------------|-------|---|
| 2 | Virtual FTP Server Tanpa SSL | Eth 0 | Address 192.168.43.10 Netmask 255.255.255.0 |
| | | Eth 1 | Address 192.168.1.1 Netmask 255.255.255.0 |
| 2 | Virtual FTP Server Dengan SSL | Eth 0 | Address 192.168.43.11 Netmask 255.255.255.0 |
| | | Eth 1 | Address 192.168.1.5 Netmask 255.255.255.0 |
| 3 | Laptop Attacker | Wifi | Address DHCP 192.168.43.X Netmask 255.255.255.0 Gateway 192.168.43.1 |

3.4.1 Anggaran Biaya

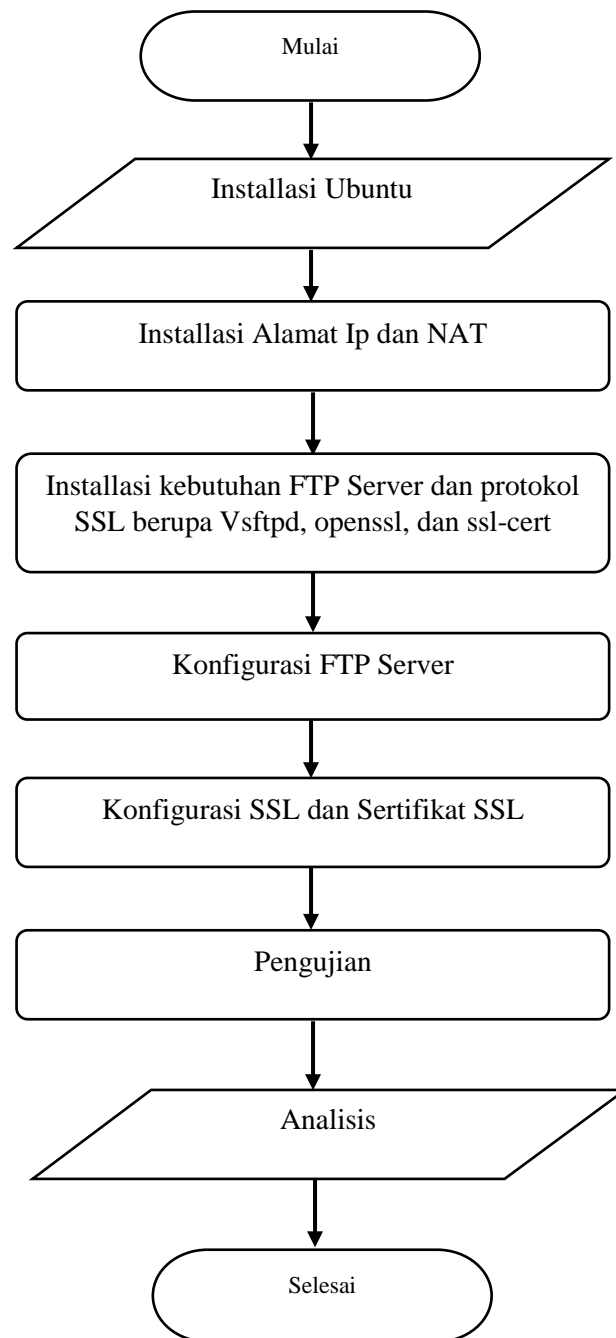
Untuk memenuhi kebutuhan dalam penelitian ini penulis melakukan perhitungan biaya yang dikeluarkan untuk penelitian mengenai analisa FTP Server dengan *protocol* SSL terhadap serangan Brute Force, sebagai berikut:

Tabel 3.2 Biaya Keseluruhan

| NO | Hardware/Software | Spesifikasi | Harga |
|----|---------------------------------|--|---|
| 1 | Laptop sebagai Server | Intel Celeron B877 Speed 1.4GHz Cache 2MB RAM 4Gb DDR3 HDD 320 GB | Rp. 3.400.000 |
| 2 | Laptop sebagai Attacker | Acer Aspire E1-431- 10002G32mn Spesifikasi: processor Type Intel Celeron Processor (1.80 GHz, 2MB Cache) RAM 2 GB DDR3 | Rp. 3.400.000 |
| 3 | Cable UTP 1.5 Meter + 2 RJ45 | Cat 5 | Kabel Rp. 3000/Meter RJ45 Rp. 500 |

3.4.2 FTP Server dengan protokol SSL yang akan diterapkan

Agar berjalannya dengan baik sebuah penelitian ini sesuai dengan apa yang diinginkan dengan baik, dibutuhkannya proses yang akan dibuat dalam bentuk diagram alir berikut:



Gambar 3.6 Flowchart langkah penerapan FTP Server

Untuk penjelasan pada gambar diatas sebagai berikut :

1. Diawali dengan melakukan installasi sistem operasi Ubuntu dalam bentuk *Command Line Interface (CLI)*.

2. Setelah selesai melakukan instalasi Ubuntu kemudian lakukan Konfigurasi pada Alamat IP dan konfigurasi NAT.
3. Setelah itu lakukan instalasi perangkat lunak yang di butuhkan FTP Server dengan SSL seperti Vsftpd, openssl, dan ssl-cert.
4. Setelah perangkat lunak telah diinstall lakukan konfigurasi terhadap FTP dan membuat sertifikat SSL.
5. Bila semua tahap telah berhasil, lakukan tahap akhir yaitu pengujian sistem yang telah dibangun lakukan pengumpulan data dan menganalisa.

3.4.3 Instalasi Ubuntu

Pada penelitian ini penulis menggunakan sistem operasi linux Ubuntu dengan mode instalasi Command Line Interface (CLI). Instalasi dilakukan dengan mengikuti proses yang telah disediakan. Seperti mengatur jenis *keyboard*, Bahasa, lokasi, alokasi partisi, dan lainnya.

3.4.4 Konfigurasi Alamat IP dan NAT

Dengan terinstallnya debian belum menentukan alamat IP didalam debian sudah terkonfigurasi, dengan begitu dilakukan penyesuaian alamat IP agar server dapat saling berkomunikasi dengan client menggunakan alamat IP ini nantinya dan mengaktifkan NAT untuk nantinya server dapat mengakses sumber internet dalam menginstall packet atau perangkat lunak seperti Vsftpd, openssl, dan cert-ssl. Seperti berikut:

Dalam mengkonfigurasi alamat IP lakukan pengeditan file *interfaces* itu sendiri dengan perintah *nano /etc/network/interfaces* kemudian akan menampilkan tampilan seperti berikut:

```

GNU nano 2.2.6      File: /etc/network/interfaces      Modified
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.1.5
    netmask 255.255.255.0
    gateway 192.168.1.1

auto eth1
iface eth1 inet static
    address 192.168.2.1
    netmask 255.255.255.0

^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell

```

Gambar 3.7 Tampilan pengalaman alamat IP

Kemudian aktifkan IP forwarding yaitu untuk NAT dapat menentukan kemana jalur dari tujuan jaringan itu sendiri dengan mengedit file *systemctl.conf* lakukan perintah seperti *nano /etc/systemctl.conf* dan hilangkan tanda # pada baris *net.ipv4.ip_forward=1*. Seperti berikut:

```

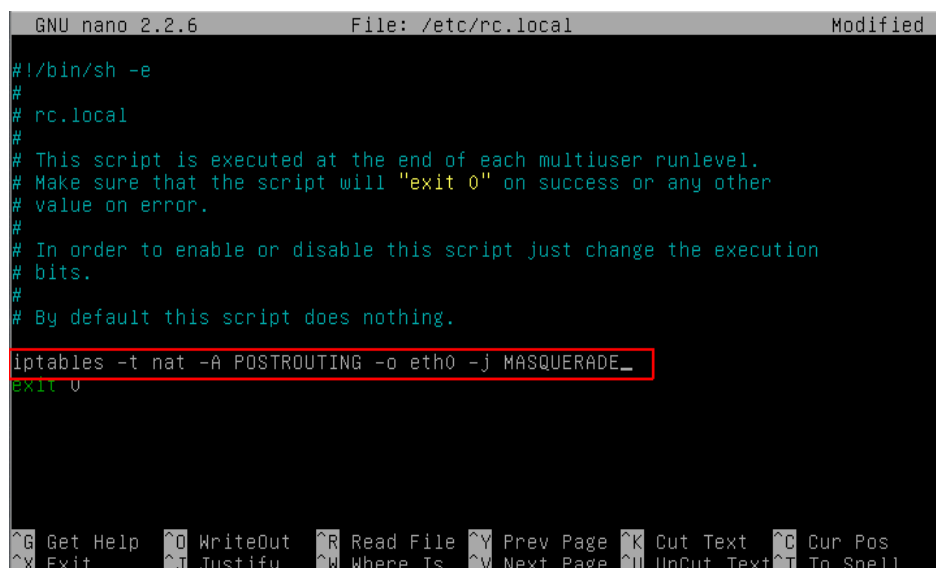
GNU nano 2.2.6      File: /etc/sysctl.conf
#####3
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1 hapus tanda pagar
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
#net.ipv6.conf.all.forwarding=1

^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell

```

Gambar 3.8 Tampilan IP Forwarding

Kemudian telah dilakukan editing pada file `systemctl.conf` dan tambahkan *Firewall* nat pada rule iptables dengan mengedit file `rc.local` berperintah `nano /etc/rc.local`. *firewall* nat ini berfungsi dimana IP paket baik yang akan keluar atau masuk diterjemahkan pada saat melewati router atau firewall seperti alamat IP sumber internet IP *Public* yaitu `eth0` ke IP *Private* client atau masquerade. Seperti berikut:



```

GNU nano 2.2.6      File: /etc/rc.local      Modified
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE_
exit 0
  
```

Gambar 3.9 Tampilan firewall NAT iptables

3.4.5 Instalasi Packet FTP Server dengan SSL

Tahap instalasi perangkat lunak dilakukan setelah `debian` menerima sumber *internet* dengan melakukan penyettingan alamat IP dan NAT. instalasi packet FTP dan SSL dilakukan agar nantinya FTP Server dengan SSL dapat di konfigurasi perintah untuk melakukan instalasi FTP Server dengan SSL yaitu dengan perintah:

```
Apt-get install Vsftpd openssl ssl-cert
```

Perintah diatas dilakukan dengan menginstall FTP sekaligus SSL dan sertifikat SSL nantinya akan membutuhkan waktu hingga instalasi selesai.

3.4.6 Konfigurasi FTP Server

Letak file utama untuk konfigurasi FTP server di Ubuntu adalah terletak pada file “Vsftpd.conf”. Buka file tersebut menggunakan text editor nano untuk melakukan konfigurasi, ketikkan perintah `nano /etc/Vsftpd/Vsftpd.conf`. lakukan konfigurasi standar seperti domain yang akan digunakan dan lainnya.

3.4.7 Konfigurasi SSL dan Sertifikat SSL

Dalam hal ini SSL telah terinstall pada server dan tahap lanjutnya yaitu membuat sertifikat SSL dengan perintah berikut:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout  
/etc/Vsftpd/ssl/ftp.key -out /etc/Vsftpd/ssl/ftp.cert
```

Setelah dilakukan hal tersebut nantinya akan diminta memasukkan beberapa data. Setelah membuat sertifikat SSL kemudian aktifkan SSL pada FTP Server agar SSL dapat bekerja terhadap FTP Server dengan mengedit file FTP Server Masuk pada `/etc/Vsftpd/Vsftpd.conf`, kemudian cari perintah `Include /etc/Vsftpd/tls.conf` dan hilangkan tanda `#`. Seperti berikut:


```

GNU nano 2.7.4 File: /etc/proftpd/proftpd.conf
#
# Alternative authentication frameworks
#
#Include /etc/proftpd/ldap.conf
#Include /etc/proftpd/sql.conf
#
# This is used for FTPS connections
#
Include /etc/proftpd/tls.conf

```

Gambar 3.10 Tampilan file Vsftpd.conf

Kemudian setelah mengaktifkan SSL untuk FTP Server lakukan beberapa konfigurasi untuk mengarahkan dimana letak dari sertifikat SSL yang akan digunakan FTP Server nantinya dengan mengedit file `tls.conf` yang berada pada folder Vsftpd. Seperti berikut:

```
# nano /etc/Vsftpd/tls.conf
```

Kemudian cari dan ubah beberapa perintah sesuai dengan berikut:

```

TLSEngine on
TLSLog /var/log/tls.log
TLSProtocol SSLv23
TLSEOptions NoCertRequest
TLRSACertificateFile /etc/Vsftpd/ssl/ftp.cert
TLRSACertificateKeyFile /etc/Vsftpd/ssl/ftp.key
TLSVerifyClient off

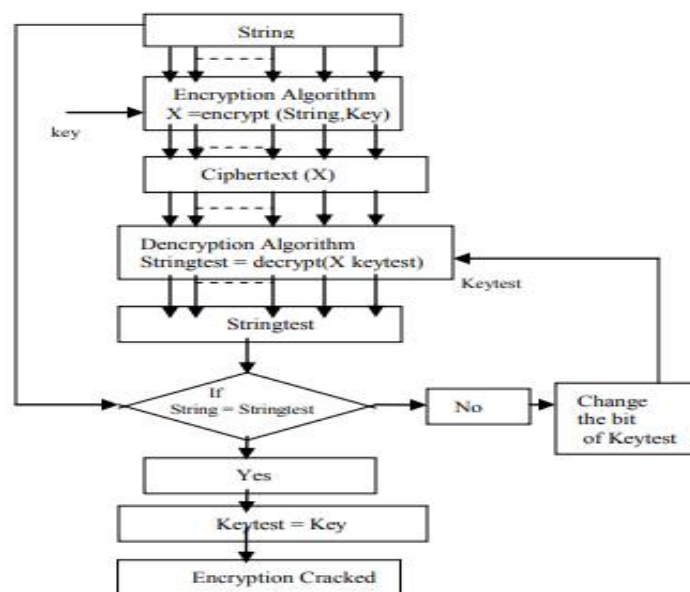
```

Pada perintah diatas dapat dilihat pada perintah yang berwarna biru menandakan letak dari sertifikat SSL yang digunakan untuk FTP Server.

3.4.8 Pengujian

Dalam penelitian ini penulis melakukan pengujian dengan menggunakan sebuah serangan yang dilakukan menggunakan perangkat lunak Xhydra dimana Xhydra ini adalah sebuah tool yang berbasis GUI (*Graphical User Interface*) yang berfungsi sebagai pemecah login password menggunakan teknik *brute force*. Aplikasi ini mendukung berbagai protokol login seperti HTTP, FTP, telnet, SMB, POP3 dan aplikasi lainnya yang membutuhkan proses autentikasi. Aplikasi ini mendukung kamus data (*dictionary*) yaitu kumpulan dari kata-kata yang akan digunakan Xhydra. Xhydra menggunakan Algoritma Brute Force yaitu algoritma yang memecahkan masalah dengan sangat sederhana, langsung, dan dengan cara yang jelas/lempang. Penyelesaian permasalahan *password cracking* dengan menggunakan algoritma Brute Force akan menempatkan dan mencari semua kemungkinan *password* dengan masukan karakter dan panjang *password* tertentu tentunya dengan banyak sekali kombinasi *password*.

Cara kerja dari algoritma Brute Force sendiri yaitu seperti berikut:



Gambar 3.11 Tampilan cara kerja dari Algoritma Brute Force

Sumber : Neeraj Kumar(2011)

Berdasarkan gambar 3.11 diatas, diperoleh cara kerja dari Algoritma Brute Force yaitu :

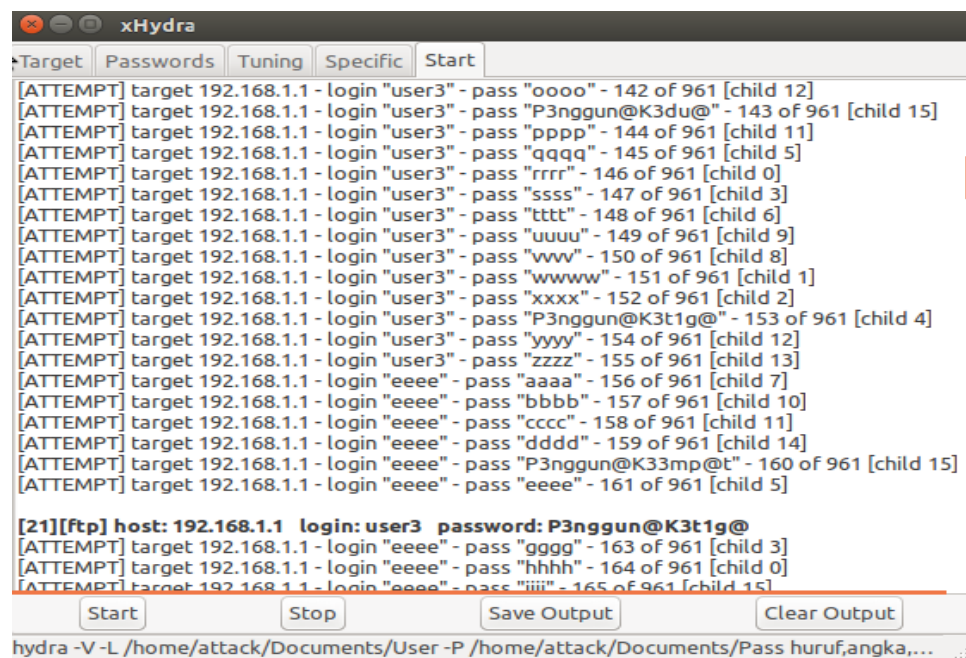
1. *String Plain text* dienkripsi menggunakan *cipher key*
2. *Chipertext X* menggunakan algoritma tertentu untuk mendapatkan enkripsinya.
3. Misalkan kunci yang digunakan "*Keytest*" sebagai hasil dari algoritma untuk dekripsi.
4. Kemudian diperoleh hasil "*String test*"
5. *String* asli dari *plain text* dibandingkan dengan "*String test*". Jika ditemukan kesesuaian maka *keytest* menjadi kunci dan akhirnya algoritma pun terbongkar. Jika tidak, 1 bit dari *keytest* akan berubah dan sekali lagi *stringtest* akan di *generate* kembali.

Dalam pengujiannya nantinya akan dilakukan penyerangan menggunakan perangkat lunak Xhydra. Xhydra dapat berjalan dalam *mode single user* atau mencoba masuk pada akun pengguna tunggal dengan mencoba kombinasi password yang berbeda atau dengan mencoba daftar kombinasi user/password dari file. Aplikasi ini akan memindai *host* untuk layanan yang dikenal dan dapat dengan mudah dimodifikasi untuk *break-in* layanan *custom* lain yang membutuhkan *login* interaktif dari sebuah username dan password. Pada pengujian ini digunakan jumlah pengguna FTP Server sebanyak 5 pengguna atau akun FTP Server dengan jumlah user list pada username dan password list

sebanyak 30 user dan password yang berbeda-beda tiap penggunaanya yang nantinya diharapkan mendapatkan hasil yang diinginkan.

Nantinya pengujian FTP Server ini menggunakan dari yang namanya monitoring wireshark untuk membantu penulis dalam menganalisa Xhydra melakukan serangan Brute Force Password Attack.

Berikut bagaimana Xhydra bekerja dalam melakukan serangan Brute Force Password Attack :



```

xHydra
+Target Passwords Tuning Specific Start
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "oooo" - 142 of 961 [child 12]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "P3nggun@K3du@" - 143 of 961 [child 15]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "pppp" - 144 of 961 [child 11]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "qqqq" - 145 of 961 [child 5]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "rrrr" - 146 of 961 [child 0]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "ssss" - 147 of 961 [child 3]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "tttt" - 148 of 961 [child 6]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "uuuu" - 149 of 961 [child 9]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "vvvv" - 150 of 961 [child 8]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "www" - 151 of 961 [child 1]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "xxxx" - 152 of 961 [child 2]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "P3nggun@K3t1g@" - 153 of 961 [child 4]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "yyyy" - 154 of 961 [child 12]
[ATTEMPT] target 192.168.1.1 - login "user3" - pass "zzzz" - 155 of 961 [child 13]
[ATTEMPT] target 192.168.1.1 - login "eeee" - pass "aaaa" - 156 of 961 [child 7]
[ATTEMPT] target 192.168.1.1 - login "eeee" - pass "bbbb" - 157 of 961 [child 10]
[ATTEMPT] target 192.168.1.1 - login "eeee" - pass "cccc" - 158 of 961 [child 11]
[ATTEMPT] target 192.168.1.1 - login "eeee" - pass "dddd" - 159 of 961 [child 14]
[ATTEMPT] target 192.168.1.1 - login "eeee" - pass "P3nggun@K33mp@t" - 160 of 961 [child 15]
[ATTEMPT] target 192.168.1.1 - login "eeee" - pass "eeee" - 161 of 961 [child 5]

[21][ftp] host: 192.168.1.1 login: user3 password: P3nggun@K3t1g@
[ATTEMPT] target 192.168.1.1 - login "eeee" - pass "gggg" - 163 of 961 [child 3]
[ATTEMPT] target 192.168.1.1 - login "eeee" - pass "hhhh" - 164 of 961 [child 0]
[ATTEMPT] target 192.168.1.1 - login "eeee" - pass "iiii" - 165 of 961 [child 15]

Start Stop Save Output Clear Output
hydra -V -L /home/attack/Documents/User -P /home/attack/Documents/Pass huruf,angka,...

```

Gambar 3.12 Tampilan cara kerja dari Xhydra Brute Force

Pada gambar 3.12 Dapat dilihat bahwa cara kerja dari Xhydra yaitu dengan mencoba semua kemungkinan yang ada pada list user dan password hingga mendapatkan hasil pencocokkan yang sama pada akun pengguna FTP Server.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Kebutuhan Spesifikasi Hardware dan Software

Sebagaimana dalam mendukung keberlangsungan penelitian ini agar penelitian ini berjalan dengan baik maka dibutuhkan beberapa perangkat keras dan lunak.

a. Kebutuhan Hardware

Hardware yang digunakan dalam mendukung penelitian analisis keamanan FTP Server dengan protokol SSL dari serangan *Brute Force* dapat di lihat dengan tabel sebagai berikut:

Tabel 4.1 Komponen Perangkat Keras

| NO | Perangkat Keras | Keterangan | Jumlah |
|-----------|------------------------|--|---------------|
| 1 | Laptop Server | Intel Celeron B877 Speed 1.4GHz Cache 2MB RAM 4Gb DDR3 HDD 320 GB | 1 unit |
| 2 | Laptop Attacker | Acer Aspire E1-431- 10002G32mn Spesifikasi: processor Type Intel Celeron Processor (1.80 GHz, 2MB Cache) RAM 2 GB DDR3 | 1 unit |

| | | | |
|---|--------------------|-----------------|----------------------------|
| | | HDD 320GB | |
| 3 | Cable UTP dan RJ45 | Cable UTP Cat 5 | 1 Meter Cable 2 RJ45 |

b. Kebutuhan Software

Untuk mendukung penelitian analisis keamanan FTP Server dengan protokol SSL dari serangan *Brute Force* dibutuhkan beberapa perangkat lunak agar sistem bekerja dengan apa yang diinginkan, adapun perangkat lunak yang dibutuhkan dapat dilihat dengan tabel berikut:

Tabel 4.2 Komponen Perangkat Lunak

| NO | Perangkat Lunak | Keterangan |
|-----------|------------------------|---|
| 1 | Sistem Operasi | Ubuntu 14.04 dipergunakan untuk sebagai sistem operasi server dan <i>attacker</i> |
| 2 | vsftpd | Dipergunakan untuk Server FTP |
| 3 | Wireshark | <i>Tool Network analyzer</i> |
| 4 | Xhydra | <i>Tool cracking password (Brute Force)</i> |
| 5 | WinSCP | Tool untuk melakukan koneksi remote FTP |

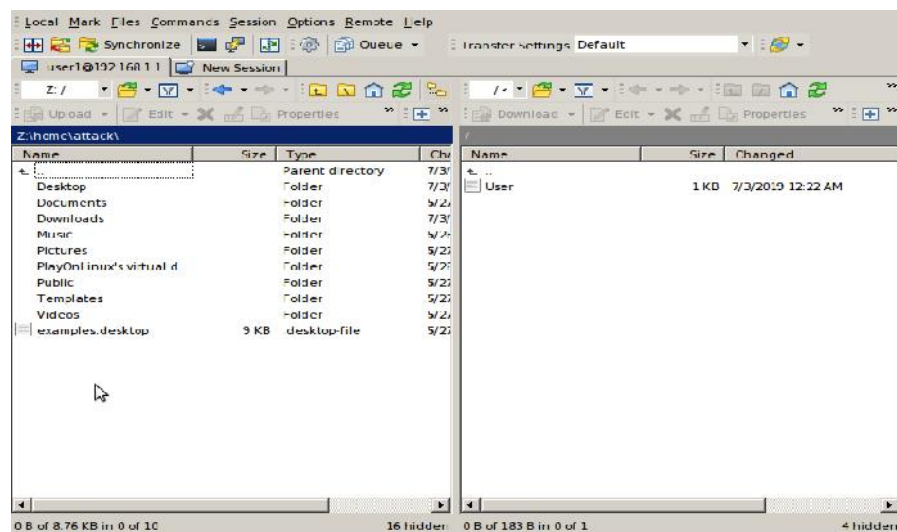
| | | |
|---|---------|---------------------------------------|
| 6 | OpenSSL | Tool untuk <i>Secure Socket Layer</i> |
|---|---------|---------------------------------------|

4.2 Pengujian dan Pembahasan

Dalam hal ini sistem yang telah dibahas dan diterapkan dengan cara sistem dioperasikan dan melakukan pengujian untuk melihat hingga sampai mana sistem yang dibangun dapat berjalan dengan baik lalu kemudian dianalisa dan sesuai dari apa yang ada pada rumusan masalah dan tujuannya.

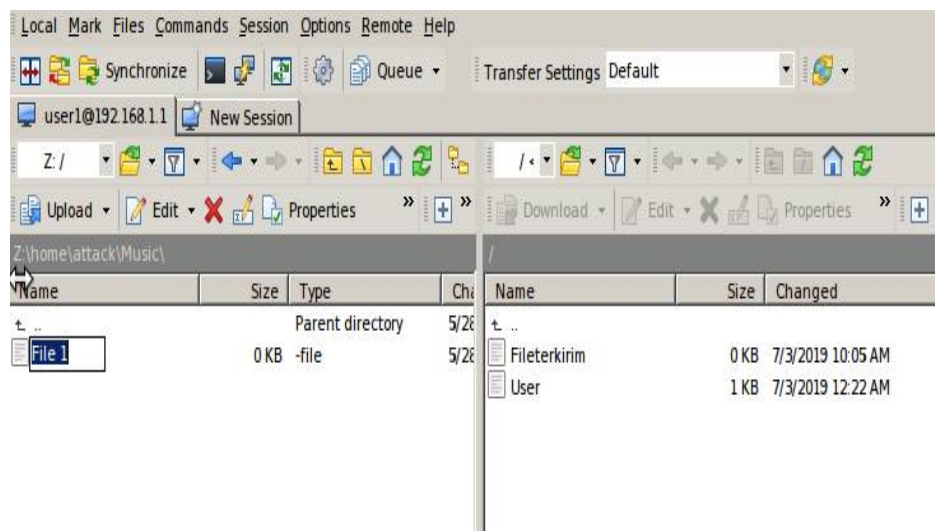
4.2.1 Pengujian FTP Server

Secara sederhananya sebelum masuk dalam tahap uji penyerangan FTP Server diuji terdahulu apakah FTP Server bekerja sesuai dengan semestinya dalam melakukan proses kerja dari FTP Server dengan mengirim (*Upload*) dan meminta (*Download*).



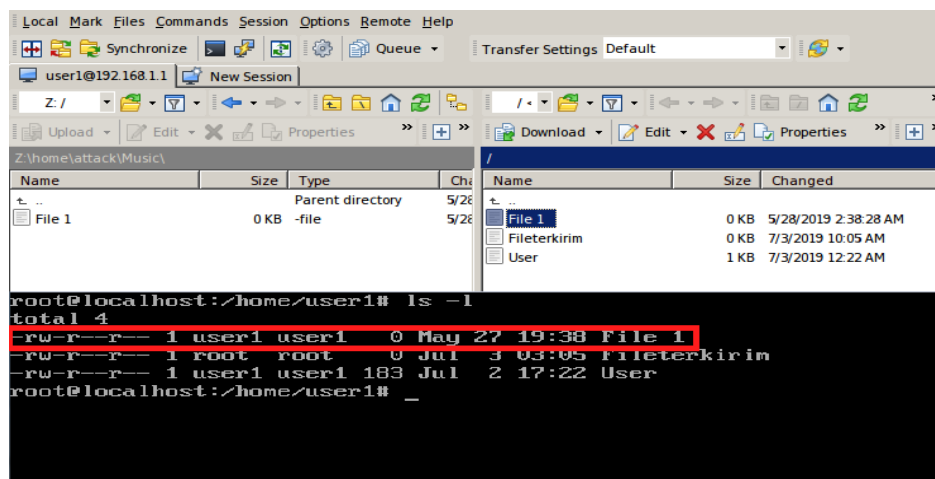
Gambar 4.1 Tampilan interface WinSCP

Pada gambar 4.1 Dapat dilihat bahwa tampilan dari tool WinSCP yang difungsikan dalam meremote FTP atau dapat dikatakan untuk memudahkan client dalam mengakses FTP Server untuk berbagi file pada server.



Gambar 4.2 Tampilan proses Mengirim (*Upload*)

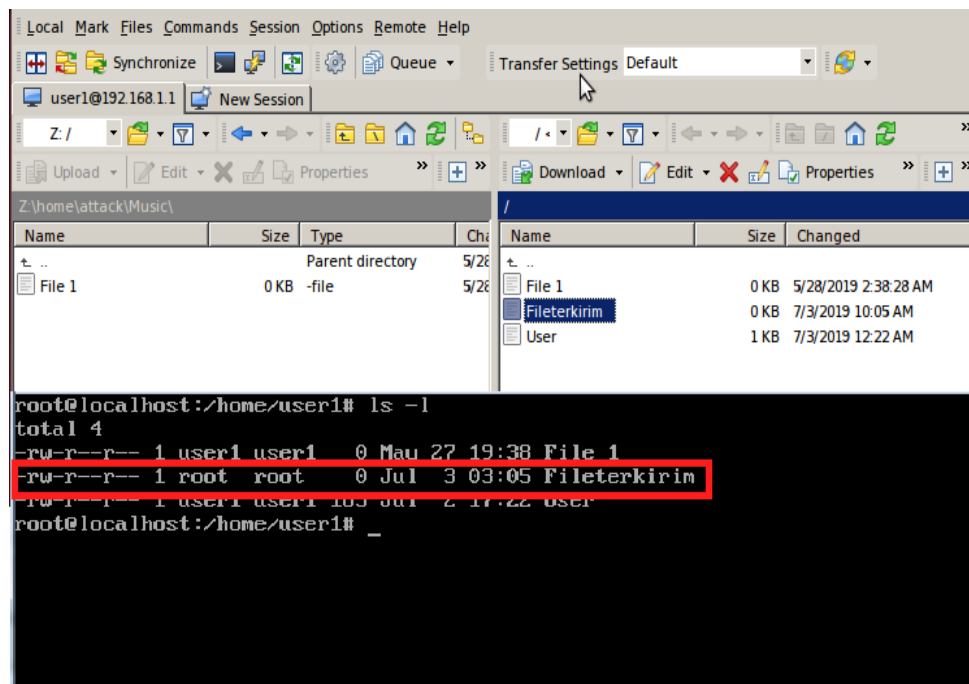
Pada Gambar 4.2 Menampilkan kegiatan atau proses dalam mengirim file kedalam server oleh user1, caranya hanya dengan memilih data contohnya nama data tersebut File1 yang akan di *Upload* kemudian tarik sebelah atau kedirektori Server untuk penyimpanan yang dikhususkan untuk pengguna user1. Berikut hasil dari proses mengirim (*Upload*):



Gambar 4.3 Tampilan hasil Proses Mengirim (*Upload*) data

Pada gambar 4.3 Menampilkan hasil proses dari mengirim data dari user 1 ke server dimana file tersebut berada pada penyimpanan yang memang dikhususkan untuk user1 itu sendiri pada gambar yang berwarna hitam adalah tampilan dari server itu sendiri dapat dilihat bahwa data tersebut berasal dari komputer user1 yang ditandai dengan owner yang berasal dari user1 yaitu (user1).

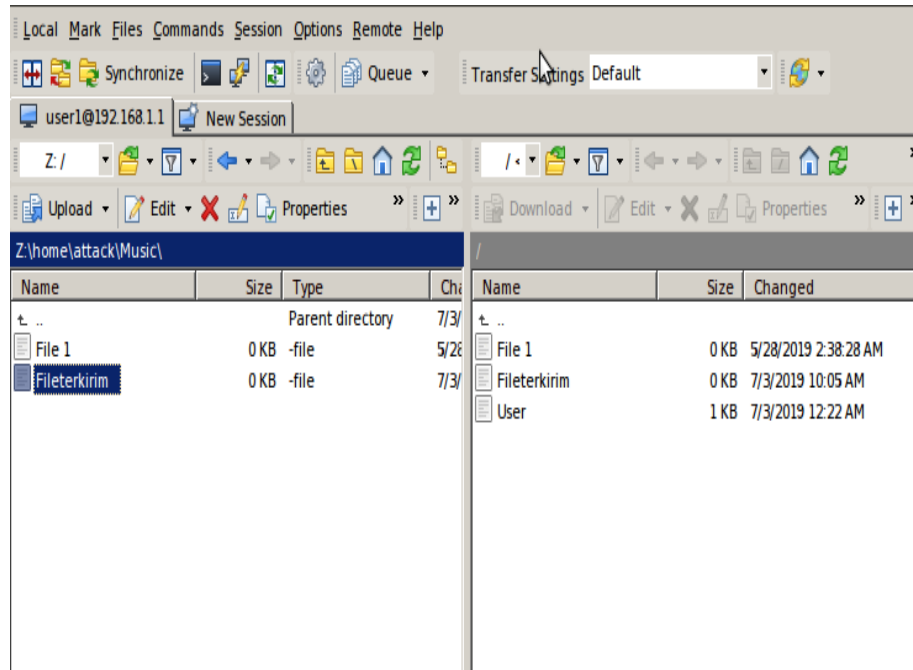
Setelah dilakukan proses mengirim (*Upload*) data maka dilakukan pengujian user1 Menerima (*Download*) data dari server seperti berikut:



Gambar 4.4 Tampilan proses menerima (*Download*) data

Pada gambar 4.4 Dapat dilihat adanya perbedaan dalam *owner* data yang dibuat oleh server itu sendiri yang ditandai dengan (*root*) dibandingkan dengan user1 yang mengirim data dengan *owner* (user1). Pada gambar pula dapat menjelaskan bahwa proses dalam melakukan penerimaan (*Download*) data sama

dengan mengirim (*Upload*) data yaitu memilih data yang akan di kirim kemudian tarik ke penyimpanan user1 seperti berikut:



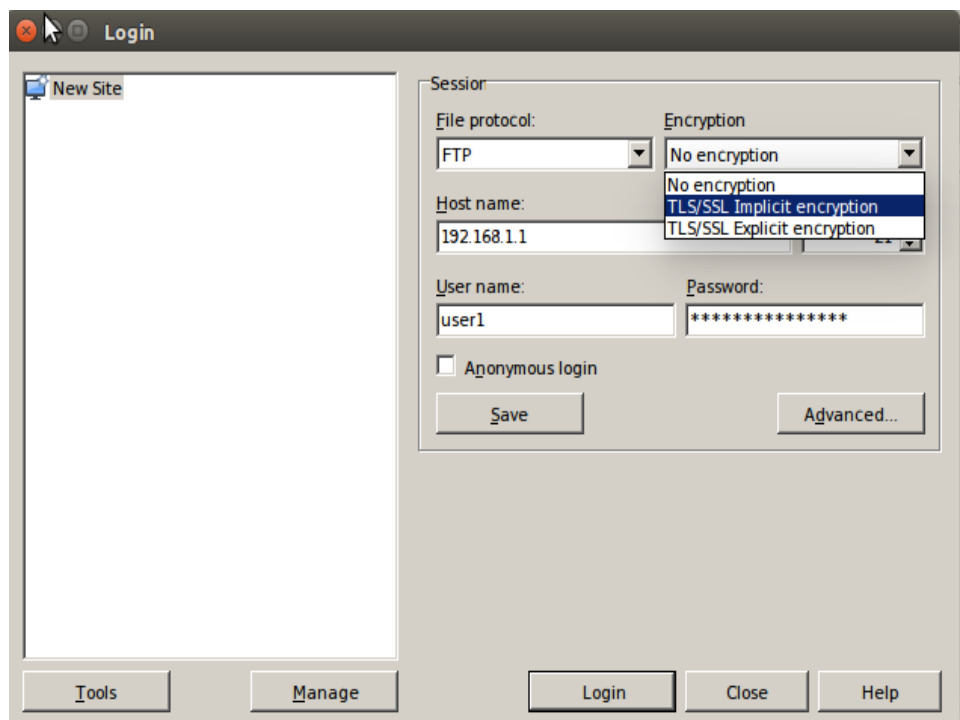
Gambar 4.5 Tampilan hasil Menerima (*Download*) data

Pada gambar 4.5 memperlihatkan tampilan bahwa data yang yang diterima telah berada pada penyimpanan user1 itu sendiri.

4.2.2 Penerapan Keamanan SSL pada FTP Server

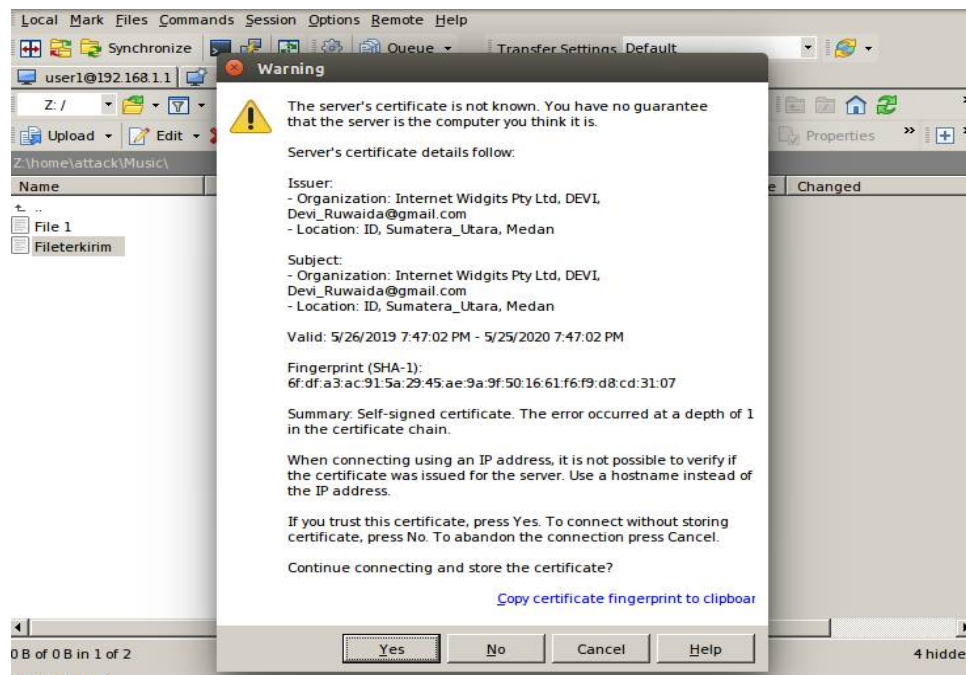
Secure Socket Layer (SSL) dipergunakan oleh FTP Server untuk mengamankan proses pertukaran data dimana proses tersebut diawali dengan prosedur *Handshaking* (jabat tangan) dengan prosedur tersebut client telah menyetujui ketentuan yang diberikan oleh server. Sebab FTP tanpa adanya keamanan FTP server hanya berjalan secara *transparent*, Karena pengiriman data tanpa adanya enkripsi *username*, *password*, dan data yang ditransfer ataupun perintah yang dikirim dapat dilakukan *sniffing* oleh pihak yang tidak diizinkan.

Untuk membedakan FTP Server yang memiliki keamanan SSL dengan yang tidak yaitu ditandai ketika awal kali melakukan autentifikasi saat login pada FTP Server seperti berikut:



Gambar 4.6 Tampilan login dari FTP Client dalam mode enkripsi SSL

Pada gambar 4.6 Menunjukkan bahwa kegiatan yang dilakukan user1 untuk masuk kedalam FTP Server dengan keamanan SSL berbeda dengan FTP Server biasa, sebab FTP Server dengan SSL harus melakukan login yang mendukung dengan enkripsi pula untuk masuk, yang fungsinya nanti agar server dapat memberikan perjanjian dengan menggunakan sertifikat dan keamanan untuk pertukaran data nantinya.



Gambar 4.7 Tampilan dari prosedur *Handshake* dengan sertifikat

Pada gambar 4.7 Dapat dilihat bahwa setelah dilakukannya login dengan menggunakan akun user maka server memberikan hak izin mengakses berupa sertifikat dari server.

4.2.3 Pengujian dan Analisa FTP Server dengan SSL dan tanpa SSL

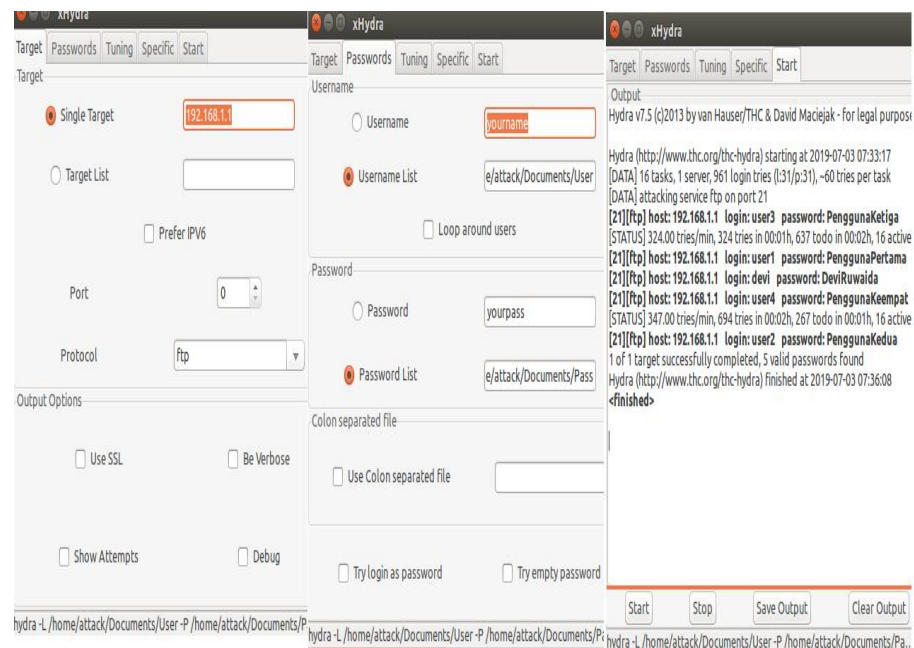
Setelah dilaluinya proses penerapan yang telah dilakukan kemudian FTP Server dengan keamanan SSL dan FTP Server tanpa SSL dilakukan beberapa pengujian dengan menggunakan *tools* untuk mengujinya baik itu menggunakan Wireshark dan menggunakan Xhydra dalam menyerang password FTP Server.

a. Pengujian dengan Wireshark

Pemanfaatan tools Wireshark dalam penelitian ini untuk melihat apa yang dihasilkan oleh monitoring trafik data terhadap penggunaan

Xhydra sebagai brute force attack dalam menyerang FTP server dengan SSL dan tanpa SSL.

Sebelum masuk pada pengujian lebih baik mengenal dahulu tool Xhydra yang dipergunakan sebagai alat untuk melakukan serangan *Brute Force Password Attack* seperti berikut:

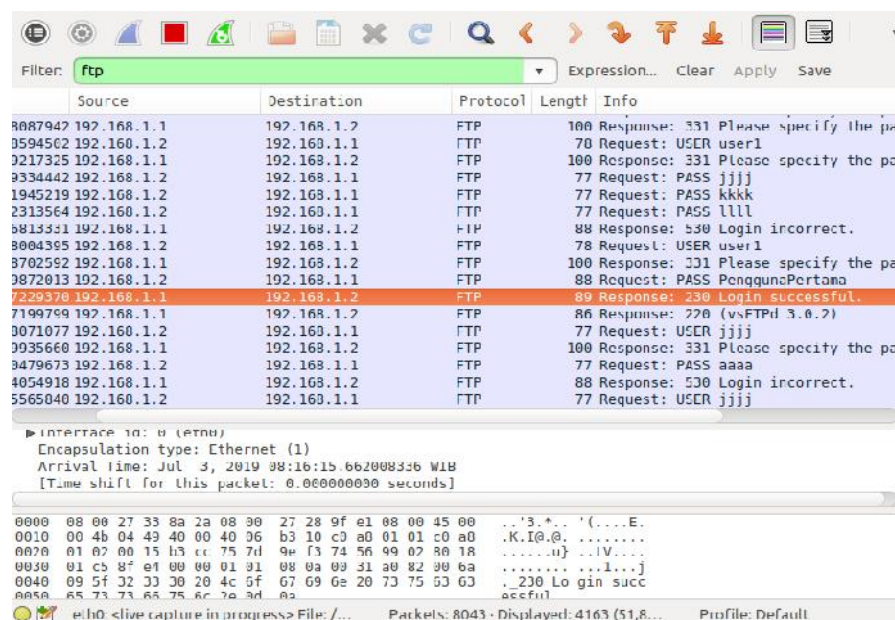


Gambar 4.8 Tampilan tool Xhydra

Pada gambar 4.8 Menampilkan apa yang ada pada tool Xhydra, Xhydra memiliki 5 menu yang dipergunakan sesuai dengan apa yang dibutuhkan penggunaanya. Dalam penelitian ini penulis hanya menggunakan 3 menu dari 5 menu yaitu menu *Target*, *Password* dan menu *Start* dimana tiap menu memiliki fungsinya masing-masing, untuk menu *Target* berisikan beberapa pilihan untuk pengguna mulai dari kolom target yang akan diserang kemudian jenis protokol yang akan diserang sebab Xhydra tidak hanya menyerang FTP saja.

Kemudian untuk menu *Password*, menu yang menyediakan kolom untuk pengguna memasukkan username dan *password* baik dalam bentuk *single* atau list. Untuk menu Start sendiri berfungsi untuk menjalankan, menghentikan, dan menyimpan keluaran dari Xhydra.

Pengujian pertama yang dilakukan yaitu dengan menguji *monitoring* lalu lintas data penyerangan *Brute Force attack* menggunakan Xhydra terhadap FTP Server tanpa adanya keamanan SSL seperti berikut:

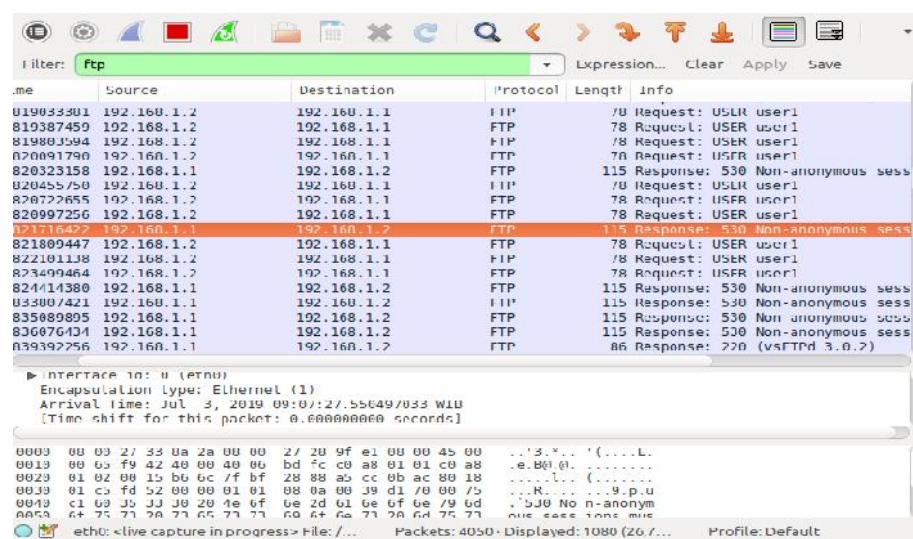


Gambar 4.9 Tampilan Monitoring serangan Xhydra FTP Server tanpa SSL

Pada gambar 4.9 Dapat dijelaskan bahwa telah dilakukannya sebuah penyerangan terhadap FTP server tanpa adanya keamanan dengan dilakukan *monitoring* menggunakan wireshark sehingga didapati cara kerja dari Xhydra *brute force password attack* yang bekerja melakukan kemungkinan percobaan tiap *username* dan *password* yang telah dibuat dalam bentuk list file yang mana isi dari list tersebut berisikan

user dan password kemungkinan dirasa ada merupakan *user* dan *password* dari FTP Server percobaan dilakukan terus menerus hingga jumlah yang telah ditentukan. Dalam penelitian ini penulis membuat sebanyak 30 list untuk *username* dan 30 list untuk *password*. *Brute force* akan melakukan pencocokkan tiap 1 dari 30 username yang ada dengan 1 hingga 30 *password* yang ada sampai mendapati username dan password yang cocok dengan user yang tersedia pada FTP Server. Keberhasilan serangan Xhydra dalam melakukan *Brute Force password attack* bila terjadinya kecocokan pada 1 user dengan password yang dicoba ditandai dengan pesan “*Login Successful*” dan bila 1 *username* tidak cocok dengan 1 *password* yang dicoba tidak sesuai dengan user FTP Server maka pesanyang ditampilkan “*Login Incorrect*”.

Pengujian kedua yang dilakukan yaitu dengan menguji *monitoring* lalulintas data penyerangan *Brute Force attack* menggunakan Xhydra terhadap FTP Server dengan keamanan SSL seperti berikut:



Gambar 4.11 Tampilan Monitoring serangan Xhydra dengan fitur
SSL

Sesuai dengan gambar 4.11 Dapat dilihat bahwa Xhydra memiliki fitur dengan protokol “FTPS” pengujian yang dilakukan terhadap FTP Server dengan SSL tidak begitu berpengaruh terhadap Xhydra dengan fitur protokol FTPS nya akan tetapi terdapat perbedaan pula pada monitoring wireshark dari pengujian satu dan dua, pada pengujian ketiga ini pesan yang diberikan “*Proceed with negotiation*” yang menandakan bahwa serangan tersebut ada terjadinya sebuah negosiasi Antara Xhydra berfitur SSL dengan FTP Server dengan SSL.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan pada bab-bab pembahasan sebelumnya dari proses konfigurasi dan dianalisis, dapat diambil beberapa kesimpulan yaitu:

1. Secara bawaannya sistem FTP hanya menggunakan metode autentikasi standar yaitu dikarena username dan password yang dikirim dalam bentuk tidak terenkripsi.
2. *File Transfer Protocol* (FTP) server membutuhkan *Secure Socket Layer* (SSL) untuk mengamankan dalam komunikasi pertukaran data sebab FTP yang digunakan tanpa adanya SSL beresiko tidak aman.
3. Sebuah FTP Server dengan SSL, Client dan server menegosiasikan sebuah koneksi dengan menggunakan sebuah prosedur *handshaking* (jabat tangan). Selama handshake ini, clien dan server menyetujui berbagai parameter digunakan untuk menetapkan keamanan koneksi.
4. FTP Server dengan keamanan SSL sudah dapat dikatakan mampu mengamankan data akun dari serangan brute force, ini terbukti dari percobaan yang dilakukan menggunakan xhydra dengan tambahan fitur SSL pula.

5.2 Saran

Pada penelitian ini penulis menemukan saran-saran yang perlu untuk pengembangan selanjutnya adalah:

1. Melakukan pengujian tidak hanya menganalisa keamanan *Secure Socket Layer* (SSL) bagi FTP saja akan tetapi menambah keamanan *Secure Socket Host* (SSH) untuk uji kelayakan keamanan untuk FTP.
2. Penambahan modul lain yang mendukung kinerja IDPS untuk membantu efisiensi kerja seperti DHCP Server dan DNS Server.

DAFTAR PUSTAKA

- Arman, Molavi, zaini. (2017). Rancang Bangun Pengamanan FTP Server dengan Menggunakan Secure Sockets Layer. Palembang: Jurnal Teknologi Integrasi.
- Andrian, Yudhi, and Purwa Hasan Putra. "Analisis Penambahan Momentum Pada Proses Prediksi Curah Hujan Kota Medan Menggunakan Metode Backpropagation Neural Network." Seminar Nasional Informatika (SNIf). Vol. 1. No. 1. 2017.
- Azmi, Fadhillah, and Winda Erika. "Analisis keamanan data pada block cipher algoritma Kriptografi RSA." CESS (Journal of Computer Engineering, System and Science) 2.1: 27-29.
- Barus, S., Sitorus, V. M., Napitupulu, D., Mesran, M., & Supiyandi, S. (2018). Sistem Pendukung Keputusan Pengangkatan Guru Tetap Menerapkan Metode Weight Aggregated Sum Product Assesment (WASPAS). Jurnal Media Informatika Budidarma, 2(2).
- Batubara, S., Wahyuni, S., & Hariyanto, E. (2018, September). Penerapan Metode Certainty Factor Pada Sistem Pakar Diagnosa Penyakit Dalam. In Seminar Nasional Royal (SENAR) (Vol. 1, No. 1, pp. 81-86).
- Dhany, H. W., Izhari, F., Fahmi, H., Tulus, M., & Sutarman, M. (2017, October). Encryption and decryption using password based encryption, MD5, and DES. In International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017) (pp. 278-283). Atlantis Press.
- Erika, Winda, Heni Rachmawati, and Ibnu Surya. "Enkripsi Teks Surat Elektronik (E-Mail) Berbasis Algoritma Rivest Shamir Adleman (RSA)." Jurnal Aksara Komputer Terapan 1.2 (2012).
- Fachri, B. (2018). Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif. Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika), 3, 98-102.
- Fuad, R. N., & Winata, H. N. (2017). Aplikasi keamanan file audio wav (waveform) dengan terapan algoritma RSA. InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 1(2), 113-119.
- Ginting, G., Fadlina, M., Siahaan, A. P. U., & Rahim, R. (2017). Technical approach of TOPSIS in decision making. Int. J. Recent Trends Eng. Res, 3(8), 58-64.
- Hafni, Layla, and Rismawati Rismawati. "Analisis faktor-faktor internal yang mempengaruhi nilai perusahaan pada perusahaan manufaktur yang terdaftar di BEI 2011-2015." Bilancia: Jurnal Ilmiah Akuntansi 1.3 (2017): 371-382.

- Halawa, Satukan. (2016). Perancangan Aplikasi Pembelajaran Topologi Jaringan Komputer Untuk Sekolah Menengah Kejuruan (Smk) Teknik Komputer Dan Jaringan (Tkj) Dengan Metode Computer Based Instruction: Jurnal Riset Komputer (JURIKOM),.
- Kumar, Neeraj. (2011). Investigations in Brute Force Attack on Cellular Security Based on Des and Aes. IJCEM International Journal of Computational Engineering & Management.
- Monoarfa, Mohamad Nurul Huda, Xaverius B.N Najoan, ST.,MT,Alicia A.E Sinsuw, ST.,MT. (2016). Analisa dan Implementasi Network Intrusion Prevention System di Jaringan Universitas Sam Ratulangi. Manado: E-Journal Teknik Elektro dan Komputer.
- Pranata, Heru, Leon Andreatti, Usman Ependi. (2015). Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan. Palembang: Student Colloquium Sistem Informasi & Teknik Informatika.
- Prihasmoro, Sukma Ageng, Yuliana Rachmawati, Erfanti Fatkhiyah. (2014). Simulasi Sistem Deteksi Penyusup Dalam Jaringan Komputer Berbasis Web Interface Serta Pencegahan Untuk Meningkatkan Keamanan. Yogyakarta: Jurnal JARKOM.
- Rosmala, Dewi, M. Djalu Djatmiko, Budiman Julianto. (2012). Implementasi Aplikasi Website E-Commerce Batik Sunda Dengan Menggunakan Protokol Secure Socket Layer (SSL). Jurnal Informatika.
- Rouesch, Martin. (1999). Snort – Lightweight Intrusion Detection for Networks. USA: USENIX Association.
- Ruwaida, Devi, Dian Kurnia. (2018). Rancang Bangun File Transfer Protocol (Ftp) Dengan Pengamanan Open Ssl Pada Jaringan Vpn Mikrotik Di Smks Dwiwarna: Jurnal CESS (Journal of Computer Engineering System and Science).
- Sugiyono. (2016). Sistem Keamanan Jaringan Komputer Menggunakan Metode Watchguard Firebox Pada Pt Guna Karya Indonesia: Jurnal CKI On SPOT.
- Sondakh, Glend, Meicsy E. I. Najoan, ST., MT, Arie S. Lumenta, ST, MT. (2014). Perancangan Filtering Firewall Menggunakan Iptables di Jaringan Pusat Teknologi Informasi Unsrat. Manado: E-Journal Teknik Elektro dan Komputer.
- Syafuddin, M, Beni Andika, Rico Imanta Ginting. (2017). Analisis Celah Keamanan Protocol Tcp/Ip: Jurnal Ilmiah SAINTIKOM Sains dan Komputer.
- Sumartono, I., Siahaan, A. P. U., & Mayasari, N. (2016). An overview of the RC4 algorithm. IOSR J. Comput. Eng, 18(6), 67-73.
- Supiyandi, S., Hermansyah, H., & Sembiring, K. A. (2020). Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video. Jurnal Media Informatika Budidarma, 4(2), 340-346.

- Syahputra, Rizki, and Hafni Hafni. "Analisis kinerja jaringan switching clos tanpa buffer." *journal of science and social research* 1.2 (2018): 109-115.
- Tehupeiory, Nardi, Dian W. Chandra. (2016). Analisis Perbandingan Mekanisme Secure Socket Layer (SSL) dan Transfer Layer Security (TLS) pada Koneksi File Transfer Protocol (FTP) Server Ubuntu: Artikel Ilmiah Universitas K. Satya Wacana.
- Tasril, V. (2018). Sistem Pendukung Keputusan Pemilihan Penerimaan Beasiswa Berprestasi Menggunakan Metode Elimination Et Choix Traduisant La Realite. *INTECOMS: Journal of Information Technology and Computer Science*, 1(1), 100-109.
- Wahyuni, Sri. "Implementasi Rapidminer Dalam Menganalisa Data Mahasiswa Drop Out." *Jurnal Abdi Ilmu* 10.2 (2018): 1899-1902.
- Wongkar, Stefen, Alicia Sinsuw, Xaverius Najoan. (2015). Analisa Implementasi Jaringan Internet Dengan Menggabungkan Jaringan LAN Dan WLAN Di Desa Kawangkoan Bawah Wilayah Amurang II. Manado: E-journal Teknik Elektro dan Komputer.