BAB II
LANDASAN TEORI

2.1 Tinjauan pustaka

Dalam penelitian oleh Joko Triyono (2014) yang berjudul " ANALISIS PERBANDINGAN KINERJA JARINGAN VPN BERBASIS MIKROTIK MENGGUNAKAN PROTOKOL PPTP DAN L2TP SEBAGAI MEDIA TRANSFER DATA", disebutkan bahwa peneliti melakukan pengamatan terhadap VPN yang menggunakan PPTP dan L2TP sebagai metode *tunneling* dan menggunakan router mikrotik. Hasil penelitian yang didapatkan dijelaskan bahwa penggunaan jaringan VPN dapat memberikan sebuah alternatif untuk melakukan akses pada sebuah situs *web* yang berdekatan dengan dengan jaringan VPN itu sendiri. Penggunaan VPN-PPTP dianggap memiliki stabilitas kecepatan yang lebih baik dan layak digunakan unruk kepentingan *home small corporate* yang tidak membutuhkan enkripsi yang terlalu rumit. Sedangkan VPN-L2TP lebih unggul untuk digunakan dalam *corporate* skala besar yang membutuhkan kehandalan dalam melakukan enkripsi.

Sarman (2006), melakukan penelitian VPN *L2TP/IPSec* dengan menggunakan *Open Swan* untuk membangun sebuah sistem jaringan yang digunakan untuk menghubungkan komunikasi jaringan lokal dengan jaringan publik secara aman pada penelitian yang berjudul "SERVER VPN BERBASISKAN LINUX DENGAN CLIENT WINDOWS XP SP2". Peneliti merancang sebuah VPN pada sistem operasi *Linux Fedora* dengan menggunakan *Open Swan* dalam menerapkan *tunneling* L2TP/IPSec dan didapatkan bahwa hasil

penggunaan VPN L2TP/IPSec mengakibatkan data yang saling bertukar antara klien dan *server* sudah terenkasulapsi walaupun sudah dilihat dengan *wireshark* dan juga penganalisa jaringan dari *Linux Fedora* serta oleh VPN tersebut hanya mengizinkan *user* yang memiliki kunci rahasia saja selain *username* dan *password* yang boleh melakukan pembentukan *tunnel* dengan *server* sehingga dengan VPN tersebut dapat dikatakan telah memiliki keamanan yang lebih baik.

Selain itu terdapat penelitian berjudul "EVALUASI IMPLEMENTASI KEAMANAN JARINGAN VIRTUAL PRIVATE NETWORK (VPN) STUDI KASUS PADA CV. PANGESTU JAYA" (Hendriana, 2012). Penelitian tersebut menjelaskan tentang evaluasi dan pengujian VPN pada suatu perusahaan yang memiliki kantor cabang di beberapa kota yang berjauhan. Dalam penelitian tersebut protokol yang digunakan adalah *IP Security*. IPsec yang diimplementasikan kedalam *site-to-site* VPN menggunakan mekanisme *network-to-network*, sehingga perlu dilakukan konfigurasi IPsec pada masing-masing *gateway*. Untuk dapat terkoneksi, masing-masing *gateway* melakukan sinkronisasi.

Area jaringan yang dilakukan pengujian adalah VPN Kantor Pusat Yogyakarta, cabang Surabaya dan cabang Bandung. Penelitian tersebut dilakukan melalui mekanisme pengujian konektivitas VPN dengan beberapa parameter, yaitu :

1. *Packet loss*

   Eksperimen pengujian ini untuk memantau rata-rata, minimum dan maksimum *packet loss* yang melalui *tunnel* VPN

2. *Round trip time*

   Eksperimen pengujian ini untuk menghitung rata-rata dan maksimum waktu *round trip* pada *tunnel* yang ada dengan menggunakan *ping*. Hasil dari eksperimen ini sama dengan hasil *packet loss* karena *packet loss* dan *round* trip merupakan satu kesatuan tes pada perintah *ping*, karena *ping* untuk menghitung waktu statistik *round trip* dan *packet loss*. *Round trip* adalah perjalanan paket *PING* dari komputer yang digunakan untuk melakukan *PING*, kemudian ke *host server data* kembali lagi ke komputer *client*, atau secara sederhana diartikan perjalanan pulang pergi.

3. *FTP transfer*

   Eksperimen pengujian ini diharapkan bisa mengetahui waktu yang dibutuhkan untuk *transfer file* melalui *tunnel* VPN. Penelitian tentang VPN juga terdapat pada makalah yang berjudul "*Performance Evaluation of Virtual Private Network*" yang membahas tentang evaluasi kinerja VPN pada Universitas Bern dengan topologi.

Penelitian di atas dilakukan dengan pengujian *traceroute*, *packet loss*, dan *FTP transfer* pada *bandwidth* internet yang berbeda, serta evaluasi kualitas enkripsi protokol VPN *IP Security* melalui metode statistik distribusi *uniform*, fungsi acak independen, dan *chi-square*.

Pada penelitian Wahyudi (2011) yang berjudul "IMPLEMENTASI VIRTUAL PRIVATE NETWORK SERVER MENGGUNAKAN SLACKWARE 13 UNTUK KEAMANAN KOMUNIKASI DATA", dilakukan studi kasus terhadap sebuah perusahaan dengan melancarkan aksi *Man In The Middle* . Pada perusahaan, menunjukan sisi klien yang menggunakan jaringan *wireless*/*hotpsot* area, penyusup dapat menyadap data – data *user* yang terhubung dalam *access point* yang sama menggunakan teknik *arp Poisoning/Spoofing* untuk mengaktifkan serangan MITMA (*Man In The Middle Attack)* diikuti dengan *sniffing*. Resiko ini bisa terjadi ketika jalur penyerang berada di antara pengguna dan situs penyedia layanan. Dan ketika dilakukan pembentukan jaringan privat melalui jaringan publik yang sering dikenal dengan *VPN (Virtual Private Network)* membuktikan bahwa jaringan lebih sulit diakses oleh pengguna yang tidak berwenang dengan melakukan MITMA tersebut.

Kemudian pada penelitian Ralph (2011), dalam penelitian berjudul "IPSec and PPTP VPN Exploits" dijelaskan bahwa peneliti melakukan penelitian terhadap protocol IPSec dan PPTP untuk mengetahui keamanannya terhadap proses *sniffing* yang dilakukan oleh peneliti. Peneliti menggunakan *software Linux Backtrack* dalam melakukan *sniffing* dan *wireshark* dalam melakukan pembacaan lalu lintas data. Dari penlitian yang dilakukan, didapatkan hasil bahwa protokol PPTP dapat terbaca ketika dilakukan *sniffing* dengan *Linux Backtrack* serta nilai pertukaran dari autentikasi *login* yang dilakukan klien dapat terlihat oleh *wireshark*. Tetapi jika menggunakan protokol IPSec, ketika dilakukan dengan penyerangan yang sama, hal tersebut tidak dapat terbaca karena sudah

terenkapsulasi oleh protokol IPSec dan dinyatakan bahwa lebih aman dengan protokol IPSec.

2.2 Landasan teori

2.2.1 Jaringan komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas sebuah komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama. Komputer dapat berhubungan satu dengan yang lainnya secara tidak terbatas baik dengan menggunakan kabel tembaga, fiber optik, *infrared*, gelombang *microwave*, bahkan bisa juga menggunakan *satellite* (Odom, 2005).

2.2.2 Jenis-jenis jaringan komputer

2.2.2.1 LAN

LAN adalah suatu jaringan komputer dalam jarak yang dekat (dalam suatu ruangan/bangunan), seperti yang dimiliki oleh organisasi dan mempunyai kecepatan komunikasi data yang tinggi (Utomo, 2011). Komponen dari suatu LAN terdiri atas:

1. Peralatan pengkomputeran (komputer, *modem*, *printer*, *storage* dan sebagainya).
2. *Card* rangkaian (*Network Interface Card*-NIC), sebagai *port*al (pintu) saat suatu komputer dikomunikasikan dengan komputer yang lain.
3. Sistem perkabelan (kabel, *connector*, *terminator* dll), sebagai media transmisi (penghantar).
4. Hub, sebagai sentral atau *concentrator* dalam jaringan, berfungsi mengatur jalannya komunikasi dan transfer data dalam sebuah jaringan

komputer. Serta terdapat *port-port* tempat terhubungnya komputer dan perangkat dalam jaringan.

5. *Software* LAN (Sistem Operasi, seperti NOS, Windows, Windows NT, Unix, Novell dan *software* aplikasi).

2.2.2.2 WAN (Wide Area Network)

WAN yaitu jaringan komputer dengan jarak jauh yang meliputi daerah, negeri maupun negara. Dalam WAN biasanya transmisi data tidak begitu cepat karena membutuhkan biaya yang sangat tinggi untuk kecepatan transmisi data yang tinggi (seperti pemakaian kabel serat optik). (Utomo, 2011)

2.2.3 Macam-Macam Topologi Jaringan

2.2.3.1 Topologi Star

Topologi ini merupakan topologi paling dasar dimana setiap *node* mempertahankan satu jalur komunikasi langsung dengan *gateway*. Topologi ini sederhana namun membatasi jarak keseluruhan yang dapat dicapai. (Utomo, 2011)

2.2.3.2 ***Topologi Cluster/Tree***

Arsitektur topologi *cluster* lebih komplek dibandingkan dengan topologi *star*. Setiap *node* masih mempertahankan satu jalur komunikasi untuk *gateway*. Perbedaannya menggunakan *node-node* lain dalam mengirimkan data, namun masih dalam satu jalur tersebut. (Utomo, 2011)

2.2.3.3 *Topologi Mesh*

Topologi ini merupakan solusi dari topologi-topologi sebelumnya, dengan menggunakan jalur komunikasi yang lebih banyak untuk meningkatkan kehandalan sistem. Dalam sebuah jaringan *mesh*, *node* mempertahankan jalur komunikasi untuk kembali ke *gateway*. (Utomo, 2011)

2.2.4 OSI Layer

Dalam (CCDA Official Exam Certification Guide, Anthony Bruno & Steve Jordan, 2007 : Appendix B) : OSI model dikenalkan oleh *International Organization for Standardization* (ISO) pada tahun 1984, dan kembali direvisi pada tahun 1994. OSI model diciptakan untuk mengkoordinasikan standar pengembangan dalam sistem pertukaran data.OSI model menjelaskan 7 lapisan (*layer*) yang berawal dari *layer* pertama *physical connection* sampai dengan *layer* ketujuh *application layer*. Setiap *layer* menyediakan *service* kepada *layer* diatasnya misalnya *layer* 2 menyediakan *service* ke *layer* 3, melakukan fungsi utamanya masing-masing, dan menerima *service* yang diberikan dari *layer* sebelumnya. Berikut adalah tujuh *layer* pada OSI model:

1. *Physical Layer* (*OSI layer 1*)

Menggambarkan trans*port*asi dari *raw bits* melalui *physical* media. Layer ini juga menjelaskan mengenai spesifikasi *signal*, tipe media, *interface* yang digunakan, tinggi rendahnya arus listrik, *physical data rates*, dan jarak maksimum suatu data dapat ditransmisi. (CCDA Official Exam Certification Guide, Anthony Bruno & Steve Jordan, 2007 : Appendix B)

2. *Data Link Layer* (*OSI Layer 2*)

Layer ini berkaitan dengan bagaimana terjadinya *reliable transport* data pada jalur fisik. Data pada *layer* ini diubah bentuk menjadi *frame*. Tugas dari *layer* ini meliputi pengurutan *frame, flow control*, sinkronisasi, notifikasi *error*, topologi jaringan secara fisik, dan pengalamatan secara fisik. (CCDA Official Exam Certification Guide, Anthony Bruno & Steve Jordan, 2007 : Appendix B)

3. *Network Layer* (*OSI Layer 3*)

Berbeda dengan *layer* 2, *layer* 3 erat kaitannya dengan informasi *routing* dan bagaimana cara untuk menentukan jalur terbaik menuju ke tempat tujuan data dikirim. Informasi yang berada di *layer* ini sudah dimodifikasi dan disebut dengan paket. Beberapa proses yang terjadi pada *layer* 3 ini adalah *routing protocol*, pengalamatan jaringan secara *logical*, dan *packet fragmentation*. (CCDA Official Exam Certification Guide, Anthony Bruno & Steve Jordan, 2007 : Appendix B)

4. *Transport Layer* (*OSI Layer 4*)

Menggambarkan bagaimana tersedianya *reliable, transparent transport* data *segment* dari *layer* diatasnya. *Layer* ini menyediakan pengecekan *error* dan *recovery* pada penerima dan pengirim data, *multiplexing, virtual circuit*

management, dan *flow control*. (CCDA Official Exam Certification Guide, Anthony Bruno & Steve Jordan, 2007 : Appendix B)

5. *Session Layer* (*OSI layer 5*)

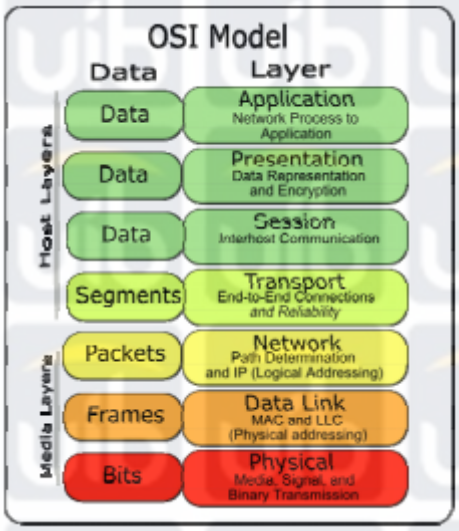
Layer ini menyediakan kontrol yang terstruktur untuk mengatur komunikasi antar aplikasi. *Layer* ini membangun, mengatur, dan menghentikan koneksi komunikasi (*session*). (CCDA Official Exam Certification Guide, Anthony Bruno & Steve Jordan, 2007 : Appendix B)

6. *Presentation Layer* (*OSI Layer 6*)

Layer ini menyediakan *service* kepada *application layer* dimana *service* itu memastikan bahwa informasi dapat terjaga selama proses transmisi. Selain itu pada *layer* ini terjadi juga proses *compression*dan *encryption* data. (CCDA Official Exam Certification Guide, Anthony Bruno & Steve Jordan, 2007 : Appendix B)

7. *Application Layer* (*OSI Layer 7*)

Pada *layer* ini *user* atau *operating system* diberikan akses ke *service* jaringan. *Layer* ini berinteraksi dengan *software* dengan cara mengidentifikasi sumber daya yang digunakan untuk komunikasi, menentukan ketersediaan jaringan dan melakukan distribusi mengenai informasi *service*. (CCDA Official Exam Certification Guide, Anthony Bruno & Steve Jordan, 2007 : Appendix B)



Gambar 2.1 OSI Layer

2.2.5 Transmission Control Protokol/Internet Protocol (TCP/IP)

Sebuah infrakstuktur jaringan adalah sekumpulan komponen fisikal dan logikal yang menyediakan dasar untuk konektivitas, keamanan, *routing*, pengaturan, akses, dan fitur integral pada jaringan.

Sering sekali, infrastuktur jaringan itu diturunkan dan dirancang. Jika jaringan terhubung ke internet, sebagai contoh, aspek-aspek tertentu seperti *Transmisi Control Protocol/Internet Protocol* (TCP/IP).

TCP/IP (*Transmission Control Protokol/Internet Protocol*) Protokol adalah spesifikasi formal yang mendefinisikan prosedur-prosedur yang harus diikuti ketika mengirim dan menerima data. Protokol mendefinisikan jenis, waktu, urutan dan pengecekan kesalahan yang digunakan dalam jaringan. *Transmission Control Protocol/Internet Protocol* (TCP/IP) merupakan protokol untuk mengirim data antar komputer pada jaringan. Protokol ini merupakan protokol yang digunakan untuk akses internet dan digunakan untuk komunikasi global. TCP/IP

terdiri atas dua protokol yang terpisah. TCP/IP menggunakan pendekatan lapisan (*layer*) pada saat membangun protokol ini. Dengan adanya pendekatan berlapis ini memungkinkan dibangunnya beberapa layanan kecil untuk tugas-tugas khusus. TCP/IP terdiri dari lima *layer*, yaitu: (Staff of Linux Journal, 2004).

1. *Layer Application*, di dalam *layer* ini aplikasi seperti FTP, Telnet, SMTP, dan NFS dilaksanakan.
2. *Layer Transport*, di dalam *layer* ini TCP dan UDP menambahkan data trans*port* ke paket dan melewatkannya ke layer internet.
3. *Layer Internet*, *layer* ini mengambil paket dari *layer* trans*port* dan menambahkan informasi alamat sebelum mengirimkannya ke *layer network interface*.
4. *Layer Network Interface*, di dalam *layer* ini data dikirim ke *layer physical* melalui *device* jaringan.
5. *Layer Physical*, *layer* ini merupakan sistem kabel yang digunakan untuk proses mengirim dan menerima data. TCP/IP dikirimkan ke setiap jaringan lokal sebagai subnet yang masing-masing *subnet* telah diberi alamat. IP yang menggunakan pengalamatan disebut dengan *IP Address*. *IP Address* ini digunakan untuk mengidentifikasi *subnet* dan *host* secara logika di dalam TCP/IP (Staff of Linux Journal, 2004).

2.2.6 IP Address

IP *address* adalah metode pengalamatan pada jaringan komputer dengan memberikan sederet angka pada komputer (*host*), router atau peralatan jaringan lainnya. IP *address* sebenarnya bukan diberikan kepada komputer (*host*) atau *router*, melainkan pada *interface* jaringan dari *host* / *router* tersebut. (Siswo Wardoyo,2014)

IP (*Internet protocol*) sendiri di desain untuk interkoneksi sistem komunikasi komputer pada jaringan paket *switched*. Pada jaringan TCP/IP, sebuah komputer diidentifikasi dengan alamat IP. Tiap-tiap komputer memiliki alamat IP yang unik, masing-masing berbeda satu sama lainnya. Hal ini dilakukan untuk mencegah kesalahan pada transfer data. Terakhir, protokol data akses berhubungan langsung dengan media fisik. Secara umum protokol ini bertugas untuk menangani pendeteksian kesalahan pada saat transfer data, namun untuk komunikasi datanya, IP mengimplementasikan dua fungsi dasar yaitu *addressing* dan fragmentasi. (Siswo Wardoyo,2014)

IPv4 adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 4. Panjangnya adalah 32-bit, dan secara teoritis dapat mengalamati hingga 4 miliar *host* komputer di seluruh dunia. Alamat IPv4 umumnya ditulis dalam notasi desimal bertitik (dotted-desimal notation), yang dibagi ke dalam empat buah oktet berukuran 8-*bit*. Karena setiap oktet berukuran 8-*bit*, maka nilainya berkisar antara 0 hingga 255. Pengalamatan IPv4 menggunakan 32 *bit* yang setiap bit dipisahkan dengan notasi titik. Contoh notasi pengalamatan IPv4:

FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF

Nilai F dirubah menjadi nilai biner (1 dan 0) 11000000.10101000.00000010.00000001. Sehingga jika dirubah dalam desimal menjadi 192.168.2.1. (Siswo Wardoyo,2014)

2.2.7 Pengertian VPN

Virtual Private Network (VPN) adalah sebuah jaringan *private* yang dibuat di atas jaringan *public* dengan menggunakan internet sebagai media komunikasinya.(Stalling 2003)

Menurut Efendi (2010), karena infrastruktur VPN menggunakan infrastruktur telUtomomunikasi umum, maka dalam VPN harus menyediakan beberapa komponen, antara lain :

a. Konfigurasi, harus mendukung skalabilitas *platform* yang digunakan, mulai dari konfigurasi untuk kantor kecil sampai tingkat *enterprise* (perusahaan besar).
b. Keamanan, antara lain dengan *tunneling* (pembungkusan paket data), enkripsi, autentikasi paket, autentikasi pemakai dan kontrol akses
c. Layanan-layanan VPN, antara lain fungsi *Quality of Services* (QoS), layanan *routing* VPN yang menggunakan BGP, OSPF dan EIGRP
d. Peralatan, antara lain *Firewall*, pendeteksi pengganggu, dan auditing keamanan
e. Manajemen, untuk memonitor jaringan VPN.

Sedangkan untuk mendapatkan koneksi bersifat *private*, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses enkapsulasi data sering disebut *tunneling*. Berikut adalah beberapa kriteria yang harus dipenuhi oleh VPN:

1. *User Authentication*: VPN harus mampu mengklarifikasi identitas klien serta membatasi hak akses user sesuai dengan otoritasnya. VPN juga dituntut mampu memantau aktifitas klien tentang masalah waktu, kapan, di mana dan berapa lama seorang klien mengakses jaringan serta jenis *resource* yang diakses oleh klien tersebut. *Address Management* VPN harus dapat mencantumkan alamat klien pada *intranet* dan memastikan alamat tersebut tetap rahasia.
2. *Data Encryption*: Data yang melewati jaringan harus dibuat agar tidak dapat dibaca oleh pihak-pihak atau klien yang tidak berwenang.
3. *Key Management*: VPN harus mampu membuat dan memperbarui encryption key untuk server dan client.
4. *Multiprotocol Support*: VPN harus mampu menangani berbagai macam *protocol* dalam jaringan publik seperti IP, IPX , dan sebagainya. Terdapat tiga protokol yang hingga saat ini paling banyak digunakan untuk VPN. Ketiga protokol tersebut antara lain adalah *Point to Point Tunneling Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP), IPSec SOCKS CIPE.

Protokol-protokol di atas menekankan pada authentikasi dan enkripsi dalam VPN. Adanya sistem otentifikasi akan mengijinkan *client* dan *server* untuk menempatkan identitas orang yang berbeda di dalam jaringan secara benar. Enkripsi mengijinkan data yang dikirim dan diterima tersembunyi dari publik saat melewati jaringan publik. Intranet merupakan koneksi VPN yang membuka jalur komunikasi pribadi menuju ke jaringan lokal yang bersifat pribadi melalui jaringan publik seperti internet. (Efendi,2010)

2.2.8 Tunneling

Tunneling adalah suatu proses mengenkapsulasi (membungkus) paket-paket atau *frame-frame* dengan header yang berisi informasi routing untuk mendapatkan koneksi *point to point* sehingga data dapat melewati jaringan publik dan dapat mencapai akhir tujuan. Tunneling protocol yang digunakan adalah sebagai berikut:

2.2.8.1 PPTP

Point-to-Point Tunneling Protocol (PPTP) merupakan teknologi baru pada jaringan yang mendukung multi protocol *Virtual Private Networks* (VPN) sehingga memungkinkan pengguna untuk mengakses jaringan suatu organisasi secara lebih aman melalui internet. Dengan menggunakan PPTP, pengguna jarak jauh dapat memanfaatkan *Microsoft Windows NT Workstation, Windows 95,* dan sistem yang mendukung PPP lainnya untuk melakukan *dial up* ke ISP lokal untuk terhubung secara lebih aman ke dalam jaringan lokal suatu organisasi dengan menggunakan internet. (Setisi,2013)

PPTP memungkinkan koneksi yang aman dan terpercaya kepada jaringan organisasi melalui internet. Hal ini sangat berguna untuk anggota organisasi yang bepergian dan harus mengakses jaringan organisasinya dari jarak jauh, untuk mengecek *email*, atau untuk melakukan aktifitas lainnya. (Setisi,2013)

Dengan PPTP, seorang pengguna dapat menghubungi nomor telepon lokal dengan menggunakan modem analog maupun modem ISDN untuk mengakses ISP dan kemudian masuk ke dalam jaringan organisasi. Setiap sesi koneksi PPTP dapat membuat koneksi yang aman dari internet ke pemakai dan kembali menuju ke jaringan organisasi. Koneksi secara lokal dari pemakai ke ISP akan menghubungkannya ke dalam hardware device *Front-End Processor* (FEP) yang dapat berada dalam kota yang sama dengan pemakai. FEP kemudian menghubungkan diri dengan NT Server yang berada di kota yang berbeda melalui WAN seperti Frame Relay atau X.25. FEP melakukan hal ini dengan mengambil paket PPP dari pemakai dan melakukan tunneling melalui WAN. Dikarena PPTP mendukung banyak protokol (IP, IPX dan NetBEUI) maka PPTP dapat digunakan untuk mengakses berbagai macam infrastruktur LAN. PPTP juga mudah dan murah untuk diimplementasikan. (Setisi,2013)

Banyak organisasi yang dapat menggunakan PPTP ini untuk menyediakan koneksi yang murah, mudah dan aman ke dalam jaringan. Hal yang terpenting dengan menggunakan PPTP adalah konfigurasi jaringan organisasi tidak perlu berubah, termasuk pengalamatan komputer-komputer di dalam jaringan intranet. WAN virtual mendukung penggunaan PPTP melalui *backbone* IP dan sangat efektif untuk digunakan. (Setisi,2013)

2.2.8.1.1 Entitas yang terlibat dalam PPTP

Untuk membangun PPTP pada umumnya dibutuhkan tiga entitas, antara lain: PPTP client, *Network Access Server* (NAS), dan PPTP server. Akan tetapi tidak diperlukan NAS dalam membuat PPTP *tunnel* saat menggunakan PPTP *client* yang terhubung dengan PPTP *server* pada LAN yang sama. (Setisi,2013)

1. PPTP Client

   Sebuah komputer yang mendukung protokol jaringan PPTP, misalnya *Microsoft Client*, dapat melakukan koneksi ke *server* PPTP dengan dua cara:

   a.Menggunakan NAS-ISP yang mendukung koneksi PPP.

   b.Menggunakan sambungan LAN dengan TCP/IP diaktifkan untuk terhubung ke *server* PPTP. PPTP client yang menggunakan NAS-ISP harus dikonfigurasi dengan modem dan perangkat VPN untuk membuat sambungan terpisah ke ISP dan *server* PPTP. Sambungan yang pertama adalah sambungan dial-up menggunakan protokol PPP melalui modem ke salah satu penyedia layanan internet. Yang kedua adalah sambungan koneksi VPN menggunakan PPTP dengan melalui modem dan koneksi ISP, ke tunnel di internet lalu ke perangkat VPN pada *server* PPTP. Sambungan yang kedua memerlukan sambungan pertama karena *tunnel* antara perangkat VPN dibangun dengan menggunakan modem dan koneksi PPP ke internet. Pengecualian untuk kedua persyaratan sambungan ini, yaitu menggunakan PPTP untuk membuat VPN di antara

komputer-komputer yang secara fisik terhubung ke jaringan LAN perusahaan *private*. Dalam skenario ini, PPTP client sudah terhubung ke jaringan dan hanya menggunakan *Dial-Up Networking* dengan perangkat VPN untuk membuat sambungan ke *server* PPTP pada LAN. Paket PPTP dari PPTP *client* secara *remote access* dan PPTP *client* pada LAN lokal akan diproses dengan cara yang berbeda. Paket PPTP dari PPTP *client* secara *remote access* akan ditempatkan pada media fisik perangkat telUtomomunikasi, sementara PPTP paket dari PPTP *client* lokal LAN ditempatkan pada media fisik *network adapter*.

2. Network Access Server (NAS)

   ISP menggunakan NAS untuk mendukung *client* yang melakukan dial dengan menggunakan protokol, seperti SLIP atau PPP untuk mendapatkan akses ke internet. Namun, untuk mendukung *client* dengan PPTP aktif maka NAS harus menyediakan layanan PPP. Server akses jaringan ISP ini dirancang dan dibangun untuk mengakomodasi banyaknya jumlah *client* yang dial-in. NAS dibangun oleh perusahaan-perusahaan seperti 3COM, Ascend, ECI Telematics, dan US Robotika yang merupakan anggota dari Forum PPTP. (Setisi,2013)

3. *PPTP Server*

   PPTP server adalah *server* dengan kemampuan *routing* yang terhubung ke jaringan private dan ke internet. Sebuah PPTP server dapat ditentukan sebagai komputer yang menjalankan Windows NT Server versi 4.0 dan Remote Access Service (RAS). PPTP diinstal sebagai protokol jaringan.

Selama instalasi, PPTP dikonfigurasi dengan menambahkan perangkat *virtual* yang disebut sebagai VPN ke RAS dan *Dial-Up Networking*. (Setisi,2013)

2.2.8.1.2 Arsitektur PPTP

Dalam Setisi (2013) disebutkan bahwa *tunneling* PPTP memiliki beberapa arsitektur didalam pembentukannya, yaitu terdiri dari:

1. *PPTP Connection and Communication*

PPP adalah *remote access protocol* yang digunakan oleh PPTP untuk mengirim data multi protokol melintasi jaringan berbasis TCP/IP. PPP mengenkapsulasi paket IP, IPX, dan NetBEUI di antara *frame* PPP dan mengirimkan paket terenkapsulasi tersebut dengan menciptakan suatu *link point to-point* antara komputer pengirim dan penerima. Sesi PPTP dimulai oleh *client* yang melakukan *dial up* NAS-ISP. Protokol PPP yang digunakan untuk membuat sambungan *dial-up* antara *client* dengan *server* akses jaringan melakukan tiga fungsi sebagai berikut:

a. Membangun dan mengakhiri sambungan fisik , PPP protokol menggunakan rangkaian yang ditetapkan dalam RFC 1661 untuk membangun dan memelihara hubungan antara *remote computer*.

b. Melakukan authentikasi, pengguna PPTP diauthentikasi oleh *client* dengan menggunakan protokol PPP.

c. Menciptakan PPP datagram, Datagram ini dienkripsi IPX, NetBEUI, atau paket-paket TCP/IP. PPP membuat datagram yang berisi satu atau lebih paket data TCP/IP, IPX, atau NetBEUI terenkripsi. Karena paket-paket jaringan dienkripsi, maka semua lalu lintas antara *client* PPP dan NAS akan menjadi aman. Dalam beberapa situasi, *remote client* dapat memiliki akses langsung ke jaringan TCP/IP, seperti halnya internet. Sebagai contoh, sebuah laptop dengan kartu jaringan dapat menggunakan internet di ruang pertemuan. Dengan sambungan IP langsung, koneksi awal PPP ke sebuah ISP menjadi tidak perlu. *Client* dapat melakukan koneksi ke *server* PPTP, tanpa terlebih dahulu melakukan koneksi PPP ke ISP.

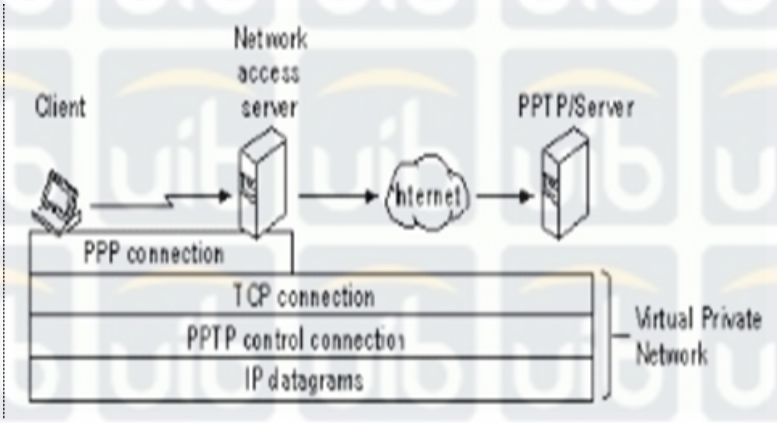
2. *PPTP Control Connection*

Protokol PPTP menentukan rangkaian pesan kontrol yang dikirim antara *PPTP-enabled client* dan PPTP *server*. Pesan-pesan control membangun, memelihara dan mengakhiri PPTP *tunnel*. Pesan-pesan kontrol dikirim dalam paket-paket control dalam datagram TCP. Satu koneksi TCP dibuat antara *client* PPTP dan *server* PPTP. Sambungan ini digunakan untuk mengendalikan pertukaran pesan.

3. *PPTP Data Transmission*

Setelah PPTP tunnel dibuat, data pengguna dikirim antara PPTP client dan PPTP server. Data yang dikirimkan dalam IP datagram berisi paket PPP. IP datagram dibuat menggunakan versi modifikasi dari protokol *Internet Generic Routing Encapsulation* (GRE). *IP*

header pengirim menyediakan informasi yang diperlukan bagi datagram untuk melintasi internet. GRE header digunakan untuk mengenkapsulasi paket PPP yang ada di dalam *IP datagram*. Paket PPP telah dibuat oleh RAS.



Gambar 2.2 Arsitektur PPTP

2.2.8.1.3 Keamanan PPTP

PPTP memperluas autentikasi dan enkripsi yang tersedia untuk keamanan komputer yang menjalankan RAS pada Windows NT *Server* versi 4.0 dan Windows NT Workstation versi 4.0 menjadi *client* PPTP di internet. PPTP juga dapat melindungi PPTP *server* dan jaringan *private*. Meskipun memiliki keamanan yang ketat, sangat sederhana untuk menggunakan PPTP dengan *firewall* yang ada. Keamanan yang tersedia pada PPTP adalah sebagai berikut: (Setisi,2013)

a. Autentikasi

Authentikasi saat awal *dial-in* mungkin diperlukan oleh sebuah ISP *network access server*. Jika authentikasi ini dibutuhkan, maka untuk *login* ke

ISP *network access server* akan menjadi lebih ketat, namun hal itu tidak berkaitan dengan authentikasi berbasis Windows NT. Setiap *client* menerapkan persyaratan untuk ISP mereka sebagai *Dial-Up Networking entry* untuk ISP tersebut.

Di sisi lain, jika Windows NT *Server* versi 4.0 dikonfigurasi sebagai PPTP *server*, ia mengontrol semua akses ke jaringan private *client*. Yakni, PPTP *server* merupakan pintu gerbang ke jaringan private *client*. Semua *client* PPTP harus memberikan nama pengguna dan *password*. Karena itu, *remote access logon* menggunakan komputer yang berjalan pada Windows NT *Server* versi 4.0 atau Windows NT *Workstation* versi 4.0 memiliki keamanan seperti *logon* dari Windows NT berbasis komputer yang terhubung ke LAN lokal.

Authentikasi dari *remote* PPTP *client* dilakukan dengan menggunakan metode authentikasi PPP yang sama dengan yang digunakan untuk panggilan langsung *client* RAS ke *server* RAS. Implementasi Microsoft dari *Remote Access Service* (RAS) mendukung skema authentikasi *Challenge Handshake Authentication Protocol* (CHAP), *Microsoft Challenge Handshake Authentication Protocol* (MSCHAP), dan *Password Authentication Protocol* (PAP). Akun pengguna dari *remote user* berada pada layanan direktori Windows NT *Server* versi 4.0 dan diatur melalui *Manager* Pengguna untuk domain. Hal ini menyediakan sentralisasi administrasi yang terintegrasi dengan jaringan private tempat akun pengguna. Hanya akun yang telah diberikan akses khusus ke jaringan melalui domain terpercaya yang akan

diijinkan masuk. Pengelolaan akun pengguna secara hati-hati diperlukan untuk mengurangi risiko keamanan.

b. *Kontrol Akses*

Setelah melakukan authentikasi, seluruh akses ke LAN private menggunakan Windows NT yang telah ada berdasarkan struktur keamanannya. Akses terhadap *resource* pada *drive* NTFS atau terhadap *resource* jaringan memerlukan perizinan, seolah-olah telah terkoneksi secara langsung ke LAN.

c. *Enkripsi Data*

Untuk enkripsi data, PPTP menggunakan RAS untuk proses enkripsi *sharedsecret*. Hal ini merujuk pada *shared-secret* karena kedua *end point* pada koneksi membagi kunci enkripsi. Pada implementasi Microsofts RAS, rahasia yang dibagi adalah *password* pengguna. PPTP menggunakan enkripsi PPP dan skema kompresi PPP. *Compression Control Protocol* (CCP) digunakan untuk menegosiasi enkripsi yang digunakan.

Username dan *password* tersedia untuk server dan disediakan oleh *client*. Kunci enkripsi dibangkitkan menggunakan hash terhadap *password* yang tersimpan pada *client* dan server. Standard RSA RC4 digunakan untuk membuat enkripsi data dengan 40- bit *session key* berdasarkan pada *password client*.

Lalu, kunci ini digunakan untuk mengenkripsi dan dekripsi seluruh data yang telah ditukar antara PPTP *client* dan *server*. Data pada paket PPP

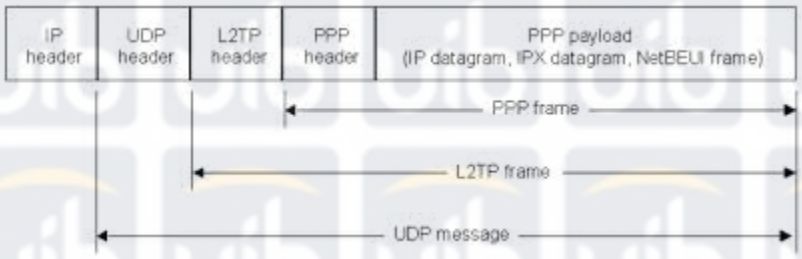
telah dienkripsi. Paket PPP berisi blok data terenkripsi yang kemudian diisi ke dalam IP datagram untuk *routing*.

d. *PPTP Packet Filtering*

Keamanan jaringan dari penyusup dapat ditingkatkan dengan melakukan PPTP *filtering* pada PPTP *server*. Ketika PPTP *filtering* telah diaktifkan, PPTP *server* pada jaringan menyetujui dan hanya mengirimkan paket PPTP saja. Hal ini mencegah seluruh tipe paket yang lain yang masuk ke dalam jaringan. Lalu lintas PPTP menggunakan *port* 1723.

2.2.8.2 L2TP (Layer 2 Tunneling Protocol)

L2TP adalah sebuah tunneling protocol yang memadukan dan mengombinasikan dua buah *tunneling protocol* yang bersifat *proprietary*, yaitu L2F (*Layer* 2 *Forwarding*) milik *Cisco Systems* dengan PPTP (*Point-to-Point Tunneling Protocol*) milik Microsoft. Namun, teknologi *tunneling* ini tidak memiliki mekanisme untuk menyediakan fasilitas enkripsi karena memang benar-benar murni hanya membentuk jaringan tunnel. Selain itu, apa yang lalu-lalang di dalam *tunnel* ini dapat ditangkap dan dimonitor dengan menggunakan *protocol analizer*. L2TP dikembangkan oleh Microsoft dan Cisco. Bisa mengenkapsulasi data dalam IP, ATM, *Frame Relay* dan X.25. (Budiadji,2009)



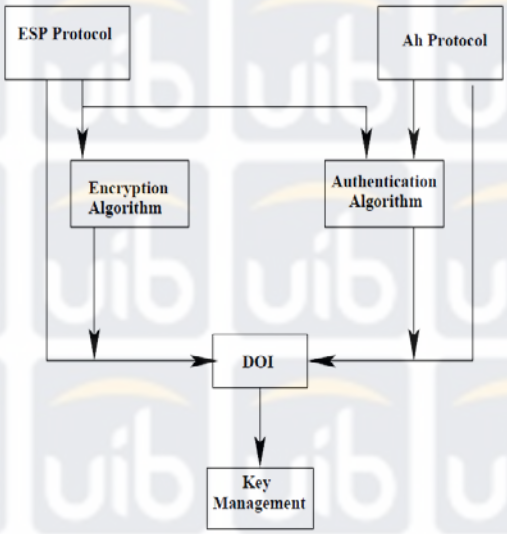
Gambar 2.3 Arsitektur L2TP

2.2.8.3 IPSec

IPSec (singkatan dari *IP Security*) adalah sebuah protokol yang digunakan untuk mengamankan transmisi *datagram* dalam sebuah *internetwork* berbasis TCP/IP (Firmansyah,2009). IPSec mendefiniskan beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA Reference Model (*internetwork layer*). IPSec melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik *tunneling* untuk mengirimkan informasi melalui jaringan Internet atau dalam jaringan Intranet secara aman. IPSec didefinisikan oleh badan *Internet Engineering Task Force* (IETF) dan diimplementasikan di dalam banyak sistem operasi. Windows 2000 adalah sistem operasi pertama dari Microsoft yang mendukung IPSec. IPSec diimplementasikan pada lapisan transport dalam *OSI Reference Model* untuk melindungi protokol IP dan protokol-protokol yang lebih tinggi dengan menggunakan beberapa kebijakan keamanan yang dapat dikonfigurasikan untuk memenuhi kebutuhan keamanan pengguna, atau jaringan.

IPSec umumnya diletakkan sebagai sebuah lapsian tambahan di dalam *stack* protokol TCP/IP dan diatur oleh setiap kebijakan keamanan yang

diinstalasikan dalam setiap mesin komputer dan dengan sebuah skema enkripsi yang dapat dinegosiasikan antara pengirim dan penerima. Kebijakan-kebijakan keamanan tersebut berisi kumpulan filter yang diasosiasikan dengan kelakuan tertentu. Ketika sebuah alamat IP, nomor *port* TCP dan UDP atau protokol dari sebuah paket datagram IP cocok dengan filter tertentu, maka kelakukan yang dikaitkan dengannya akan diaplikasikan terhadap paket IP tersebut. Layanan dari sekuritas yang disediakan oleh IPSec meliputi kontrol akses, integritas dan lain-lain seperti tesebut dibagian atas bekerja pada *IP layer* oleh karena itu layanan ini dapat digunakan oleh layer protokol yang lebih tinggi seperti TCP, UDP, ICMP, BGP dan lain-lain. IPSec DOI juga mendukung kompresi IP [SMPT 98] dimotivasi dari pengamatan bahwa ketika kompresi diterapkan dalam IPSec, hal ini akan mencegah kompresi efektif pada protokol yang lebih rendah. (Firmansyah,2009)



Gambar 2.4 Arsitektur IPSec

2.2.8.3.1 *Cara Kerja IPSec*

Untuk membuat sebuah sesi komunikasi yang aman antara dua komputer dengan menggunakan IPSec, maka dibutuhkan sebuah *framework* protokol yang disebut dengan ISAKMP/Oakley. *Framework* tersebut mencakup beberapa algoritma kriptografi yang telah ditentukan sebelumnya, dan juga dapat diperluas dengan menambahkan beberapa sistem kriptografi tambahan yang dibuat oleh pihak ketiga. Selama proses negosiasi dilakukan, persetujuan akan tercapai dengan metode autentikasi dan kemanan yang akan digunakan, dan protokol pun akan membuat sebuah kunci yang dapat digunakan bersama (*shared key*) yang nantinya digunakan sebagi kunci enkripsi data. IPSec mendukung dua buah sesi komunikasi keamanan, yakni sebagai berikut: (Firmansyah,2009)

a. Protokol Authentication Header (AH):

   Protokol ini menawarkan autentikasi pengguna dan perlindungan dari beberapa serangan (umumnya serangan *man in the middle*), dan juga menyediakan fungsi autentikasi terhadap data serta integritas terhadap data. Protokol ini mengizinkan penerima untuk merasa yakin bahwa identitas si pengirim adalah benar adanya, dan data pun tidak dimodifikasi selama transmisi. Namun demikian, protokol AH tidak menawarkan fungsi enkripsi terhadap data yang ditransmisikannya. Informasi AH dimasukkan ke dalam *header* paket IP yang dikirimkan dan dapat digunakan secara sendirian atau bersamaan dengan protokol *Encapsulating Security Payload*. (Firmansyah,2009)

b. Protokol Encapsulating Security Payload (ESP):

Protokol ini melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data. ESP juga dapat memiliki skema autentikasi dan perlindungan dari beberapa serangan dan dapat digunakan secara sendirian atau bersamaan dengan *Authentication Header*. Sama seperti halnya AH, informasi mengenai ESP juga dimasukkan ke dalam *header* paket IP yang dikirimkan. (Firmansyah,2009)

IPSec mengizinkan pengguna (administrator sistem) untuk mengontrol bagian-bagian terkecil dimana layanan keamanan diberikan (Firmansyah,2009). Sebagai contoh, salah satu dapat membuat *tunnel* enkripsi tunggal untuk membawa semua lalulintas antara dua *security gateway* atau membuat *tunnel* enkripsi terpisah yang dibuat di masing-masing hubungan TCP antara sepasang *Host* yang berkomunikasi melintasi *gateway* tersebut. Manajemen IPSec harus menggabungkan fasilitas untuk menspesifikasikan:

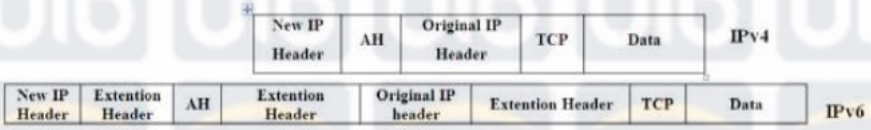
1. Layanan keamanan apa yang digunakan dan dengan kombinnasi yang seperti apa bagian sekecil apa proteksi keamanan diterapkan.
2. Algoritma yang digunakan untuk mempengaruhi keamanan berbasis kriptografi *IPSec* di design untuk memberikan keamanan trafik pada *network layer* dengan memberikan layanan utama yaitu:
   a. *Confidentially*
   b. *Integrity*
   c. *Authenticity*

d. *Anti Reply*

2.2.8.3.2 Model IPSec

Model IPSEC terdiri dari dua yaitu trans*port mode* dan *tunnel mode*.

Gambar 2.5 Transport Model



Gambar 2.6 Tunnel Model

2.2.9 Microsoft PPP CHAP Extensions Version 2 (MSCHAPv2)

Berdasarkan dokumen RFC 2759, *Microsoft PPP CHAP Extensions Version 2* (MSCHAPv2), merupakan pengembangan dari protokol otentikasi *Challenge Hanshake Authentication Protocol* (CHAP) yang dikembangkan oleh tim dari Microsoft, MSCHAP v2 memiliki kemiripan dengan protokol MSCHAPv1 dan protokol CHAP standardnya. Perbedaan mendasar antara protokol MSCHAPv1 dan MSCHAPv2 adalah, pada versi 2 menyediakan fitur *mutual authentication* antara otentikator dan *peer* (client). (Faruki,2011)

1. *Challenge Packet*

Format paket *challenge* identik dengan format paket *challenge* pada CHAP standard. Pada paket ini authenticator akan mengirimkan kepada *peer* nilai *challenge* sepanjang 16 oktet.

2. Response Packet

Format paket *Response* identik dengan format paket *challenge* pada CHAP *standard*. Format paket terdiri dari : - 16 oktet : peer *challenge*, merupakan nilai random yang dihasilkan dari sisi *peer*. - 8 oktet : nilai cadangan, harus diisi kosong / zero - 24 oktet : NT *response*, berisi password yang terenkripsi dan *username* - 1 oktet : flag, diisi dengan nilai kosong / *zero*

3. Success Packet

Format paket *Success* identik dengan format paket *Success* pada CHAP *standard*. Paket ini terdiri dari 42 oktet. Paket ini merupakan pesan *response* dari *authenticator* apabila paket *response* yang dikirimkan *peer* memiliki nilai yang sesuai. Format paket ini adalah : "S=<auth_string> M=<Message>".

4. Failure Packet

Format paket *Filure* identik dengan format paket *Failure* pada CHAP standard. Paket ini dikirimkan apabila paket *response* dari *peer* tidak ditemukan kesamaan atau tidak sesuai. Format paket ini terdiri dari "E=eeeeeeeeee R=r C=ccccccccccccccccccccccccc V=vvvvvvvvv

M=<msg>". - eeeeeeeeee, merupakan representasi nilai desimal dari pesan *error*.

5. Change-Password Packet

Format paket *Change-Password Packet* tidak sama pada CHAP dan MSCHAP v1. paket ini memungkinkan *peer* mengubah *password* pada *account* yang telah ditetapkan pada paket *response* sebelumnya. Paket ni dikirimkan oleh *peer* kepada *authenticator* apabila *authenticator* melaporkan pesan (648) ERROR_PASSWD_EXPIRED.

2.2.10 Bentuk-bentuk serangan terhadap jaringan VPN

Kegiatan dan hal-hal yang membahayakan keamanan jaringan antara lain adalah hal-hal sebagai berikut. (Purbo, 2001)

a. Probe

Probe atau yang biasa disebut *probing* adalah suatu usaha untuk mengakses sistem atau mendapatkan informasi tentang sistem. Contoh sederhana dari *probing* adalah percobaan *log in* ke suatu *account* yang tidak digunakan. *Probing* dapat dianalogikan dengan menguji kenop-kenop pintu untuk mencari pintuyang tidak dikunci sehingga dapat masuk dengan mudah. (Purbo, 2001)

b. *Scan*

Scan adalah *probing* dalam jumlah besar menggunakan suatu *tool*. *Scan* biasanya merupakan awal dari serangan langsung terhadap sistem yang oleh pelakunya ditemukan mudah diserang. (Purbo, 2001)

c. *Packet Sniffer*

Packet sniffer adalah sebuah program yang menangkap (*capture*) data dari paket yang lewat di jaringan. Data tersebut bias termasuk *user name, password*, dan informasi-informasi penting lainnya yang lewat di jaringan dalam bentuk *text*. Paket yang dapat ditangkap tidak hanya satu paket tapi bisa berjumlah ratusan bahkan ribuan, yang berarti pelaku mendapatkan ribuan *user name* dan *password*. (Purbo, 2001)

d. *Denial of Service (DoS)*

Denial of Services adalah sebuah metode serangan yang bertujuan untuk menghabiskan sumber daya sebuah peralatan jaringan komputer sehingga layanan jaringan komputer menjadi terganggu. Salah satu bentuk serangan ini adalah *'Ping Flood Attack'*, yang mengandalkan kelemahan dalam sistem *'three-way-handshake'*. (Purbo, 2001)

2.2.11 Wireshark

Wireshark merupakan salah satu *network analysis tool*, atau disebut juga dengan*protocol analysis tool* atau *packet sniffer*. *Wireshark* dapat digunakan untuk *trouble shooting* jaringan, analisis, pengembangan *software* dan *protocol*, serta untuk keperluan edukasi. *Wireshark* merupakan *software* gratis, sebelumnya. *Wireshark* dikenal dengan nama *Ethereal*. *Packet sniffer* sendiri diartikan sebagai sebuah program atau tool yang memiliki kemampuanuntuk 'mencegat' dan melakukan pencatatan terhadap *traffic* data dalam jaringan. Selama terjadi aliran data dalam, *packet sniffer* dapat menangkap *protocol data unit* (PDU), melakukan dUtomoding serta melakukan analisis terhadap isi paket berdasarkan spesifikasi RFC atau spesifikasi-spesifikasi yang lain.

Wireshark sebagai salah satu *packet sniffer* diprogram sedemikian rupa untuk mengenali berbagai macam protokol jaringan. *Wireshark* mampu menampilkan hasil enkapsulasi dan *field* yang ada dalam PDU.(*http://cisco.netacad.net*:*CCNA Exploration Network Fundamentals*). T*ools* ini hanya bisa bekerja didalam dalam jaringan melalui LAN/*Ethernet Card* yang ada di PC. Untuk struktur dari *packet sniffer* terdiri dari 2 bagian yaitu *packet analyzer* pada *layer application* dan *packet capture* pada *layer operating system* (*kernel*). Struktur dari *wireshark graphical user interface* adalah sebagai berikut : (Dinata, 2013)

a. *Command menu*

b. *Display filter specification*: untuk memfilter *packet* data

c. *Listing of captured packets*: paket data yang tertangkap oleh *wireshark*

d.*Details of selected packet header*: data lengkap tentang *header* dari suatu *packet*

e. *Packet contents*: isi dari suatu paket data

Untuk mengetahui jalur yang ditempuh untuk mencapai suatu *node, trace route* mengirimkan 3 buah paket *probe* tipe UDP dari port sumber berbeda, dengan TTL bernilai 1. Saat paket tersebut mencapai *router next-hop*, TTL paket akan dikurangi satu sehingga menjadi 0, dan *router next-hop* akan menolak paket UDP tersebut sembari mengirimkan paket ICMP *Time-to-Live Exceeded* ke *node* asal *trace route* tersebut. Dengan cara ini, pengirim *trace route* tahu alamat IP pertama dari jalur yang ditempuh. (Dinata, 2013)

2.2.12 Linux Backtrack

BackTrack adalah sistem operasi berbasis pada distribusi GNU / Linux Ubuntu yang bertujuan untuk forensik digital dan digunakan dalam pengujian penetrasi (*Hacking*). Hal ini lebih dikenal dengan istilah *Backtracking* yaitu suatu algoritma pencarian. *BackTrack* menyediakan pengguna dengan akses mudah ke banyak koleksi tool yang berhubungan dengan keamana, mulai dari *port scanner* untuk *password cracker* dan sebagainya. Dukungan untuk *Live* CD dan *Live* fungsionalitas USB memungkinkan pengguna untuk boot *BackTrack* langsung dari media portabel tanpa memerlukan instalasi, meskipun instalasi permanen ke *hard disk* juga merupakan pilihan. (Kali Linux.org)

Backtrack dibuat oleh *Mati Aharoni* yang merupakan konsultan sekuriti dari Israel yang merupakan kolaborasi komunitas. Backtrack sendiri merupakan

merger dari *whax* yang merupakan salah satu distro Linux yang digunakan untuk tes keamanan yang asal dari *whax* sendiri dari *Knoppix*. Ketika Knoppix mencapai versi 3.0 maka dinamakan dengan *whax*. *Whax* dapat digunakan untuk melakukan tes sekuriti dari berbagai jaringan di mana saja. *Max Mosser* merupakan auditor *security collection* yang mengkhususkan dirinya untuk melakukan penetrasi keamanan di Linux. Gabungan dari auditor dan Whax ini sendiri menghasilkan 300 tool yang digunakan untuk *testing security* jaringan. Auditor *security collection* juga terdapat pada knoppix. Fitur dari *backtrack* diantaranya adalah : (Kali Linux.org)

a. *Metasploit integration*
b. *RFMON wireless drivers*
c. *Kismet*
d. *AutoScan-Network*
e. *Nmap*
f. *Ettercap*
g. *Wireshark (formerly known as Ethereal) · Enumeration*
h. *Exploit Archives*
i. *Scanners*
j. *Password Attacks*
k. *Fuzzers*
l. *Spoofing*
m. *Sniffers*
n. *Tunneling*

o. *Wireless Tools*
p. *Bluetooth*
q. *Cisco Tools*
r. *Database Tools*
s. *Forensic Tools*
t. *BackTrack Services*
u. *Reversing*
v. *Misc*

2.2.13 Ettercap

Ettercap adalah alat untuk analisis protokol jaringan dan audit keamanan. Ia memiliki kemampuan untuk mencegat lalu lintas pada jaringan, menangkap password, dan melakukan menguping aktif terhadap protokol umum.

Untuk latihan ini saya akan menggunakan ARP untuk mengendus Keracunan LAN untuk *password* yang menggunakan SSL (*Hotmail*, *Gmail*, dll). ARP adalah sebuah protokol jaringan komputer *link layer* untuk menentukan *host* jaringan atau alamat *hardware* saat hanya *Internet layer* nya (IP) atau alamat *Network Layer* dikenal. Fungsi ini sangat penting dalam jaringan area lokal serta untuk lalu lintas *internetworking routing* yang di *gateway* (router) berdasarkan alamat IP ketika *router hop* berikutnya harus ditentukan.

Jadi dalam hal yang normal ARP adalah cara kita mendapatkan alamat MAC dari *Host* atau *Node* dari alamat IP. *ARP Spoofing* adalah teknik yang akan kita gunakan untuk menyerang sebuah kabel atau jaringan nirkabel. ARP *Spoofing*

memungkinkan penyerang untuk mengendus *frame* data dari LAN, kemudian memberi Anda kemampuan untuk memodifikasi lalu lintas (baik untuk mengarahkan ke komputer anda sendiri untuk men-*download* mengeksploitasi korban), atau menghentikan lalu lintas dari memasuki jaringan, atau yang spesifik komputer .

Ide di balik serangan ini adalah untuk mengirim pesan palsu ARP untuk LAN. Setiap lalu lintas pada jaringan dimaksudkan untuk alamat IP yang Anda diserang (seluruh jaringan jika Anda ingin) akan dikirim ke penyerang. Penyerang (Anda) dapat memilih untuk meneruskan lalu lintas ke *gateway* sebenarnya (*Pasif Sniffing*) atau memodifikasi data sebelum meneruskan itu (*Man in the Middle*).