ISBN: 978-602-73919-0-1

Perancangan Jaringan Keamanan *Virtual Private Network* (VPN)*Siteto Site*

Chairul Umam[1)], Emilia Roza[2)], Irfan[3)]
[1,2,3)] Program Studi Informatika, Fakultas Teknik
Universitas Muhammadiyah Prof. DR. HAMKA
Jalan Tanah Merdeka No. 6 Kampung Rambutan Ciracas Jakarta Timur DKI Jakarta 13830
Telp: (021) 8400941, Fax. (021) 87782739

Abstrak

Virtual Private Network (VPN) merupakan salah satu metode yang tepat untuk solusi keamanan jaringan dalam cangkupan Wide Area Network (WAN). VPN merupakan suatu cara memanfaatkan jaringan publik sebagai jaringan private secara aman melaluai internet. Seiring dengan maraknya penggunaan Internet, banyak perusahaan yang kemudian beralih menggunakan internet sebagai bagian dari jaringan mereka untuk menghemat biaya. Akan tetapi permasalahan keamanan masih menjadi faktor utama. Salah satu teknologi yang dapat memenuhi kebutuhan tersebut adalah Site to Site Virtual Private Network (VPN) yaitu merupakan sebuah teknologi yang memungkinkan adanya koneksi jaringan data private pada jaringan publik untuk menghubungkan antara 2 kantor atau lebih yang letaknya berjauhan, dengan menerapkan sistem enkripsi pada jaringan VPN tersebut. Dalam menggunakan VPN Site to Site, pegawai perusahaan maupun para pekerja lainnya lebih mobile bisa akses data dimana saja, serta aman dalam melakukan akses data. Pada VPN terdapat banyak protokol untuk mendukung keamanan data, salah satu protokol yang sering digunakan yaitu IPSec (Internet Protocol Security) adalah sebuah protokol yang menyediakan transmisi data terenkripsi yang aman pada network layer dalam jaringan.

***Kata kunci**: Virtual Private Network, Wide Area Network, Site to Site Virtual Private Network,IPSecurity.*

1 PENDAHULUAN

Virtual Private Network merupakan suatu jaringan komunikasi lokal yang terhubung melalui media jaringan internet. Didalam VPN terdapat perpaduan teknologi *tunneling* dan *enkripsi* yang membuat VPN menjadi teknologi yang handal untuk mengatasi permasalahan keamanan didalam jaringan. Dalam implementasinya, VPN terbagi menjadi *remote access* VPN dan *site to-site* VPN.

VPN berkembang seiring perkembangan perusahaan-perusahaan besar yang ingin tetap memperluas jaringan bisnisnya, dengan kantor cabang yang dimiliki dan perusahaan mitra kerjanya yang berada di tempat yang jauh. Perusahaan juga ingin memberikan hak akses kepada pegawai khusus sebagai fasilitas yang efektif dan efisien agar dapat terhubung ke jaringan lokal milik perusahaan tersebut di manapun mereka berada. Perusahaan tersebut perlu suatu jaringan lokal yang jangkauannya luas, tidak bisa diakses oleh sembarang orang, tetapi hanya orang yang memiliki hak akses saja yang dapat terhubung ke jaringan lokal tersebut sehingga keamanan perusahaan dapat terjaga.

Yana Hendriana (2012) dalam jurnalnya yang berjudul "*Evaluasi Implementasi Keamanan Jaringan Virtual Private Network*" menemukan masih ada celah keamanan di protokol PPTP. sehingga masih bisa di *hack* pada *username* dan *password* klien dengan serangan *man in the middle attack* melalui jaringan *hotspot* perusahaan tersebut menggunakan *backtrack.*

Amna Risky (2011) dalam penelitiannya yang berjudul "*VPN PPTP Authentication Weakness*" menemukan bahwa *VPN* yang menggunakan protokol PPTP masih bias diserang menggunakan *ARP Poisioning* dan teknik *bruteforce*.

Dari hasil penelitian kedua jurnal tersebut sistem keamanan VPN protokol PPTP yang menggunakan autentikasi MS.CHAP v2 pada windows 7 masih memiliki kelemahan dimana masih bisa di serang dengan teknik *bruteforce* menggunakan *tool* asleup pada *backtrack*.

Berangkat dari kelemahan VPN pada penelitian sebelumnya maka peneliti ingin mengetahui apakah pencurian *password* VPN bisa terjadi pada perancangan pada jurnal penelitian diatas. Peneliti juga ingin mencari solusi yang dapat dilakukan pada sisi *client* VPN untuk pencegahan pencurian *password*.

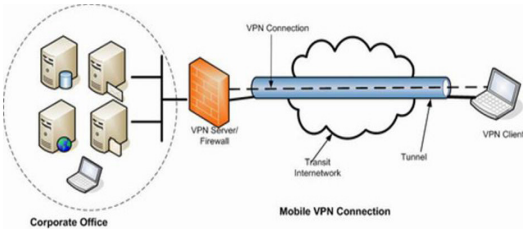
Pencegahan yang akan dilakukan untuk menghentikan pencurian *password log in user* VPN adalah dengan melakukan manajemen *password* dengan cara dibuat kombinasi huruf dan angka serta *password*-nya dibuat dari 10 digit. Hal ini bertujuan untuk menyulitkan aksi *generate key* oleh penyerang atau a*ttacker*. Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka peneliti bermaksud mengambil topik penelitian dengan judul **"Perancangan Jaringan Keamanan *Virtual Private Network* (VPN) *Site to Site*".**

2 LANDASAN TEORI

2.1 Virtual Private Network

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik. (Ahmad SS Ramadhana, 2005).

Dari cara pandang jaringan, salah satu masalah jaringan internet (IP *public*) adalah tidak mempunyai dukungan yang baik terhadap keamanan. Sedangkan dari cara pandang perusahaan, IP adalah kebutuhan dasar untuk melakukan pertukaran data antara kantor cabang atau dengan rekanan perusahaan. VPN muncul untuk mengatasi persoalan tersebut. Sebuah jaringan perusahaan yang menggunakan infrastruktur IP untuk berhubungan dengan kantor cabangnya dengan cara pengalamatan secara *private* dengan melakukan pengamanan terhadap transmisi paket data.



Gambar 1*Model VPN*

2.2 Fungsi Utama Teknologi VPN

Teknologi VPN menyediakan tiga fungsi utama untuk penggunanya. Ketiga fungsi utama tersebut antara lain:

a. Kerahasiaan

Dengan digunakannnya jaringan publik yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.

b. Keutuhan Data

Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

c. Autentikasi Sumber

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

2.3 Tipe-tipe VPN

Terdapat beragam tipe VPN, di antara yang paling populer adalah *Remote-Access* VPN dan *Site-to-Site* VPN.

a. Remote-Access VPN

Remote-Access, juga dikenal sebagai *Virtual Private Dial-Up Network* (VPDN), merupakan koneksi *user-to-LAN* yang digunakan sebuah perusahaan untuk para pekerjanya yang membutuhkan koneksi ke jaringan mereka dari berbagai lokasi remote.

b. Site-to-Site VPN

Dengan penggunaan perlengkapan *dedicated* dan enkripsi skala besar, sebuah perusahaan dapat mengkoneksikan multi site tetap melalui sebuah jaringan publik seperti *internet*.

2.4 Metode Security VPN

Guna menjamin keamanan koneksi dan data, VPN mempekerjakan beberapa metode sekuriti berikut:

a. Firewall

Firewall memberikan retriksi yang kuat di antara jaringan privat perusahaan dengan jaringan publik (internet). Kita dapat mengeset *firewall* untuk melindungi *port-port* koneksi terbuka, memeriksa tipe paket-paket mana yang perlu diteruskan, dan protokol-protokol mana yang diizinkan.

Beberapa produk VPN seperti *router-router* Cisco seri 1700 dapat kita rancang untuk memberikan kapabilitas *firewall* melalui Cisco IOS mereka. Kita biasanya sudah memiliki rancangan firewall sebelum mengimplementasikan VPN, tetapi *firewall* dapat juga kita libatkan dalam sesi-sesi VPN.

b. Enkripsi

Enkripsi (*encryption*) tidak lain proses penyandian (*encoding*) data yang diambil dari satu komputer ke komputer lain. Data disandikan ke bentuk tertentu yang tak mudah dibaca dan hanya penerima yang sah saja yang dapat mengembalikan sandi ke bentuk semula, yang dikenal dengan *decode*.

c. IPSec

Internet Protocol Security Protocol (IPSec) memberikan kapabiliti sekuriti yang lebih jauh melalui algoritma-algoritma enkripsi dan autentikasi (*authentication*).

d. AAA Server

Server-server AAA (*Authentication, Authorization and Accounting*) banyak diimplementasikan untuk memberikan akses yang lebih aman dalam sebuah *environment remote-remote* VPN. Saat request pembentukan sesi dating dari sebuah klien dial-up, request tersebut di-*proxy*-kan ke server AAA (*AAA server*).

AAA kemudian melakukan pengujian sebagai hal-hal berikut:

- Siapa Anda (*Authentication*)
- Apa yang boleh Anda lakukan (*Authorization*)
- Apa yang sebenarnya Anda lakukan (*Accounting*)

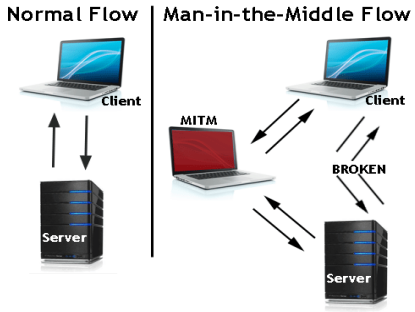
2.5 Serangan Terhadap Keamanan Jaringan Komputer

Menurut W. Stallings [William Stallings, "*Network and Internetwork Security*," Prentice Hall, 1995.] biasanya serangan terhadap keamanan jaringan VPN antara lain:

a. Man In The Middle Attack

Man in The Middle Attack atau MITM *attack* adalah serangan dimana attacker berada di tengah bebas mendengarkan dan mengubah percakapan antara dua pihak. Serangan *Man in The Middle* merupakan suatu tipe serangan yang memanfaatkan kelemahan *Internet Protocol*.

Konsep dasar serangan ini secara umum adalah penyerang berada ditengah – tengah atau diantara dua komputer yang sedang berkomunikasi, sehingga secara teknis memungkinkan penyerang untuk melihat, mengubah dan mengontrol data yang dikirim antar dua komputer tersebut, mesin penyerang secara fisik tidak harus terletak diantara dua computer, namun rute paket yang dikirimkan atau ditujukan kepada *host* lain harus melalui mesin penyerang



Gambar 2 *Serangan Man In The Middle Attack*

Ada berbagai kegiatan atau istilah kejahatan dunia maya yang termasuk dalam kegiatan *Man in the middle*, antara lain adalah:

1. *Sniffer*
   Sniffer yang juga dikenal sebagai *Network Analyzers* atau *Ethernet Sniffer* ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Dikarenakan data mengalir secara bolak-balik pada jaringan, aplikasi ini menangkap tiap-tiap paket dan kadang-kadang menguraikan isi dari RFC (*Request for Comments*) atau spesifikasi yang lain. Berdasarkan pada struktur jaringan (seperti *hub* atau *switch*), salah satu pihak dapat menyadap keseluruhan atau salah satu dari pembagian lalu lintas dari salah satu mesin di jaringan.
2. *Spoofing*
   Spoofing adalah situasi dimana seseorang berhasil menyamar sebagai user *dengan* memalsukan data dan dengan demikian mendapatkan keuntungan tidak sah.
3. *Interception*
   Merupakan ancaman terhadap *secrecy* dimana orang yang tidak berhak namun berhasil mendapatkan akses informasi dari dalam sistem komputer.
4. *Modification*
   Merupakan ancaman terhadap *integrity* dimana orang yang tidak berhak dapat mengakses maupun merubah suatu informasi.
5. *Fabrication*
   Menambahkan objek atau informasi palsu pada informasi yang asli, sehingga data atau informasi berubah.

b. Bruteforce

Menurut Wikipedia, Serangan brutal (*Brute-force attack*) adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua

kunci yang mungkin. Teknik yang paling banyak digunakan untuk memecahkan *password*, kunci, kode atau kombinasi. Cara kerja metode ini sangat sederhana yaitu mencoba semua kombinasi yang mungkin.

Sebuah *password* dapat dibongkar dengan menggunakan program yang disebut sebagai *password cracker*. Program *password cracker* adalah program yang mencoba membuka sebuah *password* yang telah terenkripsi dengan menggunakan sebuah algoritma tertentu dengan cara mencoba semua kemungkinan. Teknik ini sangatlah sederhana, tapi efektivitasnya luar biasa, dan tidak ada satu pun sistem yang aman dari serangan ini, meski teknik ini memakan waktu yang sangat lama, khususnya untuk *password* yang rumit.

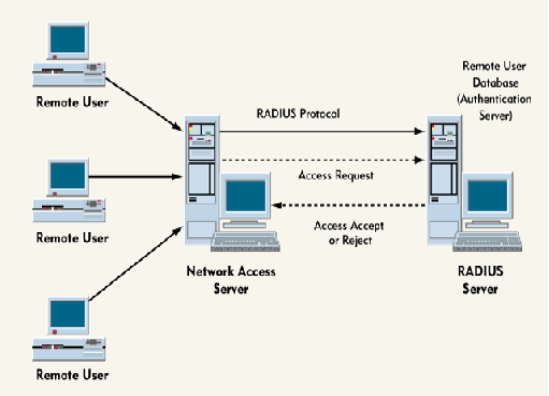
2.6 Wireshark

Wireshark merupakan salah satu dari sekian banyak *tool Network Analyzer* yang banyak digunakan oleh *Network Administrator* untuk menganalisa kinerja jaringannya terrmasuk protokol didalamnya. *Wireshark* banyak disukai karena interfacenya yang menggunakan *Graphical User Interface* (GUI) atau tampilan grafis.

Wireshark mampu menangkap paket-paket data atau informasi yang lewat dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang *tool* ini juga dapat dipakai untuk sniffing (memperoleh informasi penting seperti *password e-mail* atau *account* lain) dengan menangkap paket-paket yang lewat di dalam jaringan dan menganalisanya.

2.7 RADIUS (*Remote Authentication Dial-In User Service)*

Remote Authentication Dial-In User Service adalah sebuah protokol keamanan komputer yang digunakan untuk melakukan autentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan. Radius diterapkan dalam jaringan dengan model *client-server*.



***Gambar 3** Ilustarasi RADIUS*

koneksi user, menghitung durasi waktu dan jumlah transfer data dilakukan oleh *user*. *Software* server Radius yang digunakan dalam penelitian ini adalah Freeradius yang bersifat modular dan memiliki banyak fitur. *Freeradius* merupakan *software server* yang berbasis pada open source dan berlisensi GPL.

3 PERANCANGAN

3.1 Identifikasi Masalah

Pada penelitian VPN sebelumnya yang sudah dibahas di latar belakang masalah, masalah perancangan VPN yang terjadi adalah banyaknya serangan yang terjadi pada jaringan lokal/intranet. Salah satunya masih terdapat kelemahan VPN yang masih bisa di *hack username* dan *password* melalui serangan *Man In The Middle Attack* dan *bruteforce* di protokol PPTP. Dalam hal ini peneliti berusaha membahas cara mengamankan jaringan komputer lokal/intranet. Hal ini dimaksudkan ketika kita mengetahui metode, tingkah laku maupun jenis serangan yang dilakukan, kita dapat lebih mengantisipasi serangan-serangan tersebut. Kita pun dapat mengamankan celah-celah yang rentan untuk diserang menjadi lebih baik dan aman.

3.2 Identifikasi Perancangan

Untuk mendukung perancangan VPN *Site to Site* ini, peneliti membutuhkan hal-hal sebagai berikut:

a. Identifikasi Kebutuhan Sistem *Software*

Pada penelitian kali ini perangkat lunak (*software*) yang peneliti gunakan adalah sebagai berikut:

1. Sistem operasi *server* Mikrotik RouterOS v5.9
2. Sistem operasi *client* menggunakan sistem operasi *Windows* 8 Pro
3. Sistem operasi penyerang menggunakan sistem operasi *backtrack* 5 yang diinstal secara *virtual*dan bantuan tool untuk serangan:
   - Ettercap
   - Wireshark
   - Asleap-2.2
   - Chap2asleap.py
   - Genkeys
   - Crunch

b. Identifikasi Kebutuhan Sistem *Hardware*

Sedangkan perangkat keras (*hardware*) yang peneliti gunakan untuk penelitian ini adalah sebagai berikut:

- Mikrotik RB 1100
- Notebook Acer Aspire 4352

Setelah identifikasi kebutuhan sistem, maka sistem harus dirancang terlebih dahulu sebelum dibangun agar mengetahui bentuk sistem keamanan untuk menahan serangan *Man In The Middle Attack* dan *Bruteforce* di jaringan lokal melalui protokol PPTP.

3.3 Perancangan Sistem

Setelah identifikasi kebutuhan sistem, maka sistem harus dirancang terlebih dahulu sebelum dibangun agar mengetahui bentuk sistem keamanan untuk menahan serangan *Man In The Middle Attack* dan *Bruteforce* di jaringan lokal melalui protokol PPTP.

3.4 Perancangan PC *Server*

Kemudian selanjutnya setelah perancangan sistem yaitu melakukan perancangan PC server untuk dua buah *server* yang pertama akan dijadikan sebagai VPN site to site untuk menghubungkan beberapa perusahaan cabang atau dua mitra perusahaan, selain itu juga untuk menahan serangan *Man In The*

Middle Attack dan *Bruteforce* di protokol PPTP. Kedua adalah *RADIUSserver* yang dapat menangkap user untuk melakukan autentikasi, otorisasi, dan pendaftaran akun pengguna.

3.5 Install

a. Install PC Server

Tahap selanjutnya adalah melakukan install sistem operasi pada dua buah PC *Server*. Dimana PC *server* pertama ini diinstal mikrotik routerOS untuk VPN site to site. Selanjutnya PC *server* kedua di *install softwareFreeRadius* untuk melakukan autentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan.

b. Install Aplikasi

Selanjutnya setelah melakukan install mikrotik Router OS adalah melakukan konfigurasi VPN *Site to Site* di *winbox* yang akan menahan serangan *Man In The Middle Attack* dan *Bruteforce*. Sedangkan pada PC *server* keduaakan dilakukan install aplikasi *Free Radius*.

3.6 Setting

Setelah selesai install PC server dan aplikasi, lalu lakukan setting atau konfigurasi terhadap PC *Server*. Dimana PC *Server* yang telah di *install* Mikrotik. Konfigurasi PC *Server* ini meliputi *setting PPTP Server*, *routing*, *user VPN client*, dalam VPN *server*. Sedangkan setting PC *Server*

kedua yang telah diinstall *Free Radius* memiliki konfigurasi dan aturan yang beda.

3.7 Setting Ulang

Apabila dalam setting awal terjadi kegagalan dalam uji serangan terhadap sistem di jaringan lokal/*intranet*. Apabila hal tersebut terjadi, maka peneliti akan melakukan setting ulang terhadap konfigurasi *server* VPN dan RADIUS.

3.8 Uji Coba Serangan Man In The Middle Attack dan Bruteforce

Pada tahap ini peneliti melakukan uji coba serangan *Man In The Middle Attack* yaitu bentuk aktif menyamar dimana penyerang membuat koneksi independen dengan korban dan pesan *relay* antara mereka, membuat mereka percaya bahwa mereka berbicara langsung satu sama lain melalui koneksi pribadi, padahal sebenarnya seluruh percakapan dikendalikan oleh penyerang.

Selain uji coba *Man In The Middle Attack*, peniliti juga melakukan uji coba serangan *bruteforce*. Dimana serangan *bruteforce* adalah teknik serangan terhadap sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin. Teknik yang paling banyak digunakan untuk memecahkan *password*, kunci, kode atau kombinasi.

4 HASIL

Dari 2 kali penyerangan *Man In The Middle Attack* dan *bruteforce* VPN PPTP di perusahaan "X" dapat memperlambat waktu untuk memecahkan kode *username* dan *password* dengan waktu 5 detik dengan menggunakan kode *password* lebih dari sama dengan (≥) 8-10 digit seperti keterangan pada gambar 4.21, sedangkan dalam penelitian sebelumnya dalam jurnal Amna Risky (2011) "*VPN PPTP Authentication Weakness*" dan jurnal Yana Hendriana (2012) "*Evaluasi Implementasi Keamanan Jaringan Virtual Private Network*" langsung bisa ditembus dan dibaca *username* dan *password*nya. Akan tetapi dengan menggunakan apllikasi wireshark kita dapat memutus percobaan untuk mendapat *password login* VPN korban.

5 SIMPULAN

1. Model jaringan VPN Site to Site akan mewujudkan akses data yang aman bagi perusahaan serta membuat jaringan yang terjamin keamanannya dari serangan *Man In The Middle Attack* dan *Bruteforce*.
2. Menggunakan *password* 8-10 digit akan dapat memperlambat serangan *hacker* untuk membaca *username* dan *password* selama 5 detik. Dengan waktu selama 5 detik, admin harus mampu memutus serangan tersebut dengan *Wireshark*.

KEPUSTAKAAN

[1] Aris Wendy, Ramadhana SS Ahmad, 2005. *Membangun VPN Linux Secara Cepat*, Andi Yogyakarta.

[2] Ariyus, Dony. 2007. *Instruction Detection System*. Yogyakarta : ANDI OFFSET

[3] `Athailah. 2013. *MikroTik untuk Pemula*. Jakarta: MediaKita.

[4] Andi, 2005. *Seri Buku Pintar: Menjadi Administrator Jaringan Komputer.* Yogyakarta

[5] Hendriana, Yana. 2012. *Evaluasi Implementasi Keamanan Jaringan Virtual Private Network.* Jakarta: Universitas Islam Negeri Syarif Hidayatullah

[6] Pleeger, Charles. 2003. *Security In Computing Third Edition*. United State Of America: Pearson Education

[7] Stallings, William. 2007. *Komunikasi & Jaringan Nirkabel*. Diterjemahkan oleh: Dimas Aryo Sasongko, S.T. Jakarta: Erlangga

[8] Pratama, I Putu Agus Eka. 2014. *Handbook Jaringan Komputer*. Bandung: Informatika Bandung.

[9] Risky,Amna. 2011. *VPNPPTP Authentication Weakness.* Jakarta: Universitas Islam Negeri Syarif Hidayatullah.

[10] Stallings, William. 2000. *Komunikasi Data dan Komputer: Jaringan Komputer*. Diterjemahkan oleh : Thamir Abdul Hafedh Al Hamdany. B,Sc., M.Sc. 2002. Jakarta: Salemba Teknika.

[11] Tanenbaum, Andrew S. 1996. *Jaringan Komputer Edisi Bahasa Indonesia Jilid 2*. Diterjemahkan oleh: Ir. Gurnita Priatna. 1997. Jakarta: Prenhallindo.