ANALISIS PERBANDINGAN KINERJA VPN PPTP, ANONYMOUS PROXY DAN SSH TUNNEL PADA ISP DAN INTERNET SHARING

Erfan Wahyudi[1], Ery Rizal Hidayat[2], Muhammad Zohri[3], Ahmad Subki[4]
STMIK Mataram[1,3,4]
Universitas Amikom Yogyakarta[2]
Universiti Kebangsaan Malaysia[3]
Universitas Islam Indonesia[1,4]
erfan.wahyudie@gmail.com

Abstrak – Penggunaan internet sebagai sarana untuk mentransfer suatu informasi memiliki tantangan tersendiri karena sifatnya yang terbuka untuk umum atau semua kalangan, maka masalah kerahasiaan dan otentikasi dari informasi yang diterima dan dikirim juga bersifat terbuka. Ada beberapa cara yang digunakan untuk mengatasi masalah tersebut termasuk penggunaan PPTP VPN, Proxy dan SSH Tunnel yang menggunakan server luar negeri dan bebas tanpa batasan. Dalam paper ini, penulis melakukan pengujian simulasi dengan menguji kinerja dan keamanan jaringan untuk mendapatkan informasi yang diinginkan tentang apa yang terbaik dalam membypass akses terbatas ke semua situs di internet. Hasilnya, berdasarkan parameter troughput pada file gambar, VPN PPTP memiliki nilai troughput lebih besar 1,2 % dari ISP Cobralink; Proxy Anonymus lebih besar 11%; sedangkan SSH Tunnel lebih besar 23% dibandingkan saat menggunakan ISP Cobralink. Diagram perbandingan performa menunjukan bahwa terdapat perbedaan performa pada tiap-tiap metode yaitu VPN PPTP, Proxy Anonymous dan SSH tunnel pada koneksi ISP Cobralink. Penulis menggunakan paket internet dengan bandwith 250 Kbit/s dan burst max 380 Kbit/s. Burst adalah bandwitdh tambahan di atas max-limit yang mungkin didapatkan dalam kondisi tertentu sedangkan burst max adalah speed maksimal yang mungkin didapatkan saat kondisi burst. Penggunaan proxy HTTP/HTTPS maupun SOCK5 pada ISP Cobralink dapat meningkatkan rata Burst.

Kata kunci: Linux, VPN, Proxy Anonymous, SSH Tunnel, VPS

1. LATAR BELAKANG

Meskipun saat ini akses internet mudah di dapatkan di seluruh dunia, tapi terdapat beberapa situs yang terbatas untuk negara-negara tertentu saja. Tidak mengherankan, ini membuat pembajakan lebih tinggi di negara yang tidak bisa mengakses konten tersebut. Pemakainan internet sebagai sarana jaringan public untuk mendapatkan maupun mengirimkan suatu informasi mempunyai resiko tersendiri karena internet terbuka untuk umum, maka masalah kerahasiaan dan autentikasi atas informasi yang diterima dan dikirim pun juga terbuka..

Beberapa cara untuk mengatasi permasalahan diatas antara lain menggunakan VPN PPTP, Proxy, dan SSH *Tunnel* yang menggunakan *server* di luar negara yang terbebas batasan. Virtual *Private network* Point to Point Tunneling Protocol(VPN PPTP) merupakan *protocol* jaringan yang memungkinkan pengamanan transfer data dari *remote client* (*client* yang berada jauh dari *server*) ke *server* pribadi perusaaan dengan membuat sebuah VPN melalui TCP/IP (Ariyus, 2008), Proxy *server* adalah computer *server* atau program computer yang bertindak sebagai computer lainya untuk melakukan request terahadap content dari internet atau intranet, sedangkan *Secure Shell* (SSH) memungkinkan user SSH untuk mengirimkan paket data yang telah di bungkus atau di enkapsulasi di jaringan protokol *Hypertext Tranfer Protocol*(HTTP) menggunakan protokol *Secure Socket Layer* (SSL) sebagai *payload* ,dan *Tunneling* adalah mengirimkan data melalui koneksi yang telah terbentuk.

Berdasarkan permasalahan tersebut penulis tertarik untuk mengajukan penelitian dengan judul "Analisis Perbandingan Kinerja VPN PPTP, Proxy Anonymous, dan SSH Tunnel Pada ISP dan Internet Sharing"

2. LANDASAN TEORI

a. VPN (Virtual Private Network)

VPN dapat di artikan suatu jaringan private yang mempergunakan sarana jaringan komunikasi public yaitu internet dengan memakai tunneling protocol dan prosedur pengamanannya.

VPN dapat digunakan pada jaringan yang telah ada, seperti internet, maka VPN dapat memfasilitasi transfer data yang bersiafat sensitive secara aman melealui jaringan public. VPN juga dapat menyediakan solusi yag fleksibel seperti pengaman komunikasi antara remote user dengan *server* sebuah organisasi tampa harusa memikirkan di mana letak remote user tersebut.

Vpn dapat menggunakan kedua bentuk kriptografi, yaitu kriptografi kunci simetris dan kiptografi kunci public. Kiptografi kunci simetris

biasanya lebih efisien dan membutuhkan ongkos pemrosesan yang lebih murah bila dibandinkan dengan kriptografi kunci public. Olehkarena itu kriptografi kunci simetri lebih sering di gunakan untuk mengenkripsi bagian terpenting dari data yang di kirim melalui VPN.

Algoritma yang umum digunakan untuk mengimplementasi kriptografi kunci simetri meliputi *Digital Encryption Standard* (DES), *Triple* DES (3DES), *Advanced Encryption Standard* (AES), *Blowfish*, RC4, *International Data Encryption Algorrthm* (IDEA), dan *Hash message Authentification Code* (HMAC) versi *Message Digest* 5 (MD5) dan *Secure Hash Algorithm* (SHA-1). Sedangkan Algoritma yang umunya digunakan untuk algoritma kunci public adalah meliputi RSA, *Digital Signature Agorithm* (DSA), dan *Elliptic Curve* DSA (EDBSA).

b. **Point to Point Protocol (PPTP)**

PPTP merupakan protocol yang mengijinkan hubungan *Point-to-Point Protocol* (PPP) melewati jaringan IP, dengan membuat Virtual *Private network* (VPN). Teknologi jaringan PPTP merupakan pengembangan dari *remote access Point-to-Point Protocol* yang dikeluarkan oleh *Internet Enginering Task Force* (IETF). PPTP merupakan protocol jaringan yang merubah paket PPP menjadi IP datagram agar dapat di transmisikan melalui internet. PPTP juga dapat digunakan pada jaringan *private* LAN-to-LAN.

PPTP terdapat sejak dalam sjak dalam system operasi Windows NT *server* dan Windows NT Workstation versi 4.0. Komputer yang berjalan dengan sisitem operasi tersebut dapat menggunakan protokol PPT dengan aman untuk terhubung dengan *private network* sebagai klien dengan remote access melalui internet. PPTP juga dapat digunakan oleh computer yang terhubung dengan LAN untuk membuat VPN melalui LAN.

Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya *public- swithed telephone network* (PSTNs) untuk membangun VPN.Pembangunan PPTP yang mudah dan berbiaya murah untuk digunakan secara luas, menjadi solusi untuk remote users dan mobile users karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet. Akan tetapi tidak diperlukan *network* access *server* dalam membuat PPTP tunnel saat menggunakan klien PPTP yang terhubung dengan LAN untuk dapat terhubug dengan *server* PPTP yang terhubung pada LAN yang sama

c. Proxy

Proxy dan *server* proxy adalah dua istilah yang digunakan oleh pengguna internet intermediate. Proxy merujuk ke sebuah situs web, yang dapat digunakan untuk memblokir informasi. Dengan kata lain, tanpa batas, Anda dapat memperoleh akses kepada informasi melalui Internet dengan menggunakan proxy websites. Proxy website ini hanya disebut sebagai proxy. *Server* proxy adalah *server* antara yang menangani berbagi data antara klien dan *server*. Data apapun dibagi antara klien dan *server* harus melewati proxy *server*. Proxy website dirancang untuk membodohi *server* proxy.

Hampir semua dinas dan instansi pendidikan menginstal proxy *server*, yang berfungsi sebagai *Firewall*. Koneksi internet ke komputer dalam berbagai bangunan disediakan hanya melalui *server* proxy. Setiap bagian dari informasi yang melewati *server* proxy, adalah log. Dengan cara ini, petugas yang dapat mengontrol akses internet mereka bawahannya atau siswa. *Firewall* dipasang di *server* proxy, yang membatasi akses ke berbagai situs web. Dalam sebagian besar kasus, banyak dikenal hiburan dewasa dan situs-situs yang diblokir oleh *server* proxy (Thomas, 2005).

Proxy merupakan komputer *server* yang bertindak sebagai perantara antara komputer yang kamu gunakan dengan internet. Tidak seperti VPN, proxy *server* tidak selalu melakukan enkripsi data yang dikirim maupun diterima komputer melalui jaringan internet, inilah mengapa akses proxy sedikit lebih cepat dibandingkan akses VPN karena tidak melakukan enkripsi (Risanuri, 2013).

d. SSH Tunnel

SSH adalah protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan. Banyak digunakan pada Sistem Operasi berbasis Linux dan Unix untuk mengakses akun shell, SSH dirancang sebagai pengganti Telnet dan shell remote tak aman lainnya, yang mengirim informasi, terutama kata sandi, dalam bentuk teks sederhana yang membuatnya mudah untuk dicegat. Enkripsi yang digunakan oleh SSH menyediakan kerahasiaan dan integritas data melalui jaringan yang tidak aman seperti Internet (Reza, 2013).

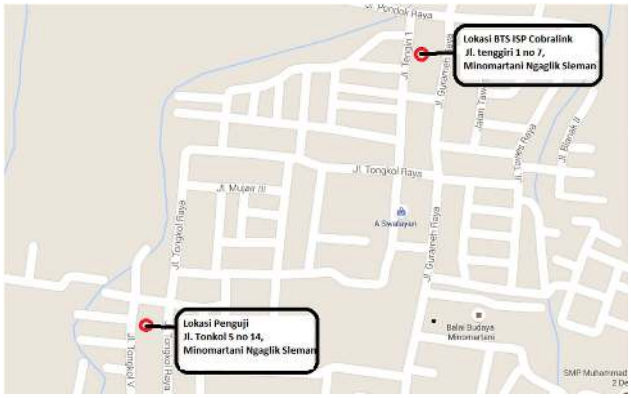
Protocol SSH ini memiliki banyak fungsi, selain fungsi tunneling yang sering kita gunakan, kita juga bisa menggunakan SSH untuk SFTP, SOCKS4/5 proxy atau bisa juga kita gunakan untuk mengatur VPS atau hosting milik kita khususnya VPS dengan OS Linux seperti CentOS.Untuk menggunakan tunneling menggunakan SSH ini kita bisa mengguankan SSH *client* seperti Bitvise Tunnelier ataupun Putty untuk sistem operasi Windows (IlmuHacking, 2014).

Tunneling sendiri adalah mengirimkan data melalui koneksi lain yang sudah terbentuk melalui enkapsulasi paket data. Dalam kasus https, data dalam protokol HTTP di-enkapsulasi (dibungkus) dalam protokol SSL sebagai payload. Enkapsulasi juga terjadi dalam layer model TCP/IP, yaitu data pada layer yang lebih atas menjadi payload dan di-enkapsulasi dengan protokol pada layer di bawahnya.

3. ANALISIS DAN PERANCANGAN

Pada tahap ini dibahas mengenai analisis kondisi jaringan ISP Cobralink saat ini, Perancangan sistem dan metode pengujian yang akan digunakan untuk membandingan kinerja VPN PPTP, Proxy *Anonymous*, SSH tunnel serta ISP Cobralink Minomartani. Perancangan dimulai dengan perencanaan topologi jaringan, *software* dan *hardware* yang digunakan, serta metode pengujian yang akan digunakan.

ISP Cobralink Cobralink menggunakan jaringan WAN RT/RW net, yaitu dengan menggunakan BTS sebagai Repreater dimana penulis melakukan pengujian di tempat yag berbeda dengan lokasi BTS yang ada. Berikut denah atau peta BTS ISP Cobralink Minomartani dan lokasi pengujian.



Gambar 1. Jarak BTS Cobralink dan Lokasi Pengujian

Informasi secara singkat tentang bentuk jariangan WAN yang ada pada ISP Cobralink Minomartani adalah sebagai berikut :

Tabel 1. Jaringan WAN pada ISP Cobralink Minomartani

IP BTS	10.10.254.30
IP Gateway VLAN pada Penulis	10.18.200.129
MAC address	02:42:68:6c:71:54

Simulasi uji peforma dilakukan dengan cara melakukan *download* file dari *server* ke *client* dengan menggunakan metode *client* terkoneksi jaringan yang berbeda yaitu VPN PPTP, Proxy, dan SSH tunnel.Untuk proses pengambilan data akan dilakukan penangkapan paket- paket yang lewat pada sisi *client* dengan mengunakan perintah curl.

Terdapat dua parameter yang akan di ambil dalam pengambilan data, yaitu *throughput* dan *transfer time* . *Throughput* merupakan banyaknya bit yang diterima pada suatu node per satuan waktu, sedangkan waktu transfer adalah waktu yang dibutuhkan untuk mengirimkan suatu data dari satu node ke node yang lain. File yang di *download* dari *server* berupa file Gambar dengan format JPG dengan ukuran 2448 x 3264 besarnya 2.30 MB, dan file Suara dengan format MPEG Layer 3 (mp3) berukuran 3.12 MB dengan bitrate 320 kbps. Perbedaan Jenis file dan ukuran file ini bertujuan untuk mengamati hubungan antara jenis file dan ukuran file dengan parameter-parameter uji. Sedangkan untuk pengambilan data pada masing-masing parameter uji coba dilakukan seanyak 5 kali untuk setiap kapasitas file pada masing-masing konfigurasi jaringan.

Agar dapat diperoleh kesimpulan yang tepat, maka dilakukan pembatasan yaitu menggunakan satu buah(1) *Virtual Private Server* (VPS) yang telah di konfigurasi VPN PPTP *server*, Proxy *Server*, dan OpenSSH *server* dan terdapat batasan bandwith dalam tiap-tiap paket biling ISP Cobralink.

Sedangkan Simulasi Uji Keamanan akan dilakukan dengan cara sinffing menggunakan aplikasi, ettercap dan wireshark pada suatu user yang menggunakan metode VPPN PPTP, Proxy anynomous, dan SSH tunnel, cara ini umum digunakan para penyerang untuk mencuri *password* maupun data atau informasi pada suatu situs internet. Tujuan penyerang untuk menyadap (*Sniffing*) akses informasi pada korban.Pada metode ini dimana akan terjadi proses pecencurian data dengan cara menyadap paket yang dikirim oleh user melalui jaringan lan agar penyerang dapat mendapat informasi yang di inginkan.

4. HASIL PENGUJIAN

a. Pengujian Performa

Pengambilan data dilakukan pada saat klien yang ber sistem operasi linux Backbox 4.4 melakukan hubungan dengan virtual private server (VPS) dengan menggunakan VPN PPTP, Proxy server, dan SSH server. Paket yang dikirim berupa Gambar

dengan format JPG dengan ukuran 2448 x 3264 besarnya 2.30 MB, dan file Suara dengan format MPEG Layer 3 (mp3) berukuran 3.12 MB dengan bitrate 320 kbps. Dengan menggunakan perintah cURL dimana nanti akan bisa dilihat Throughput yang dihasilkan ketika menggunakan VPN PPTP, Proxy, dan SSH Tunnel dan Throughput yang dihasilkan ketika menggunakan jaringan ISP Cobralink saja, serta waktu transfer yang dibutuhkan untuk mentransfer suatu file baik dari Klien ke Server maupun dari Server ke Klien.

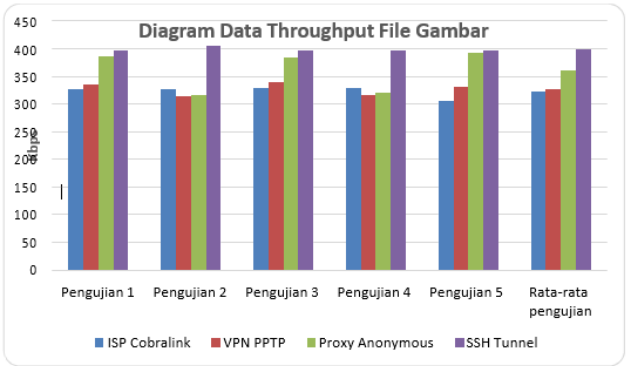
Gambar 2. Pengambilan nilai troughput

Gambar 3. Pengambilan nilai transfer time

Dapat dilihat pada gambar di atas bahwa dengan perintah curl –o [link] dapat melakukan proses *download* sehingga file yang ter*download* terlihat prosess *download* dari besar file, rata-rata *download*, total waktu dan waktu yang dibutuhkan dan terlihat juga kecepatan saat proses *download* berlangsung. Pada penggunaan proxy dan SSH tunnel diperlukan aplikasi proxychain agar cURL dapat melewati proxy baik tipe HTTP maupun SOCK5 proxy.

1) Analisis Pengukuran Dengan Data Berupa Gambar

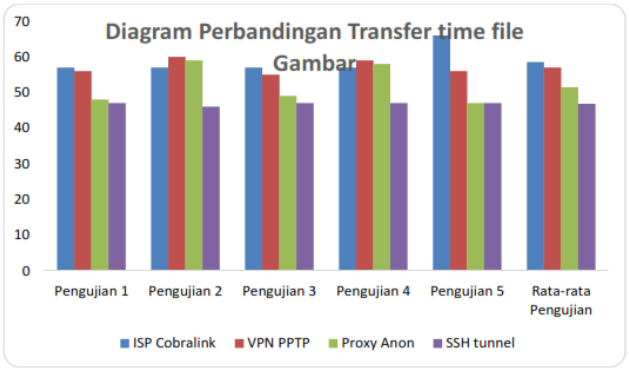
Pada pengukuran ini yaitu berupa file gambar dengan format JPG dengan ukuran 2448 x 3264 besarnya 2.30 MB dari *server* ke *client* sebanyak lima kali. Data paket nilai *throughput* yang digunakan di ambil dari *average download* pada perintah cURL berupa *bytes per second* sehingga perlu dikalikan 8 untuk memperoleh satuan *bit per second*. Data yang diamati pada hasil *download* pada perintah cURL.



Gambar 4. Diagram Data Troughput File Gambar

Dari Diagram diatas dapat dilihat pada pengujian 1 sampai 5 nilai ketika hanya mengunakan koneksi dari ISP Cobralink memiliki rata-rata throughput 323.5140 Kbit/sec , saat menggunakan VPN PPTP tidak memiliki pengaruh yang signifikan yaitu 327.5859 Kbit/sec yang berarti terjadi kenaikan throughput sebesar 1.2 % saat menggunakan VPN PPTP, sedangkan saat menggunakan Proxy Anonymous dan SSH Tunnel throughput mengalami kenaikan. Pada proxy Anonymous throughput menjadi 360.4968 Kbit/sec yang berarti mengalami kenaikan sebesar 11 % dibandingkan dengan kondisi normal internet Cobralink dan SSH tunnel mengalami kenaikan yang signifikan yaitu 23% pada throughput rata-rata 398.7796 Kbit/sec.

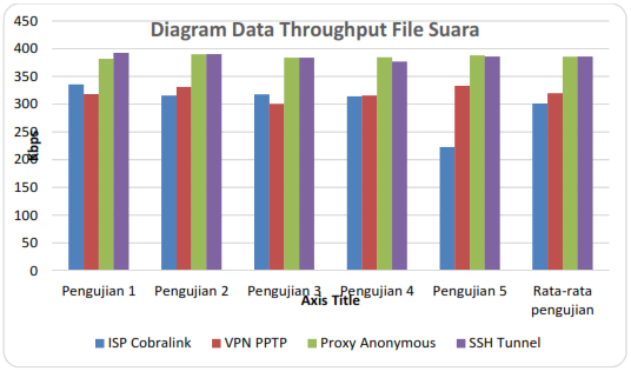
Begitu juga untuk waktu transfernya, dari 5 kali pengujian didapatkan rata ketika menggunakan VPN PPTP 2% sedikit lebih cepat dibandingkan dengan jaringan ISP Cobralink yaitu 57 detik sedangkan jaringan ISP Cobralink 58.5 detik, sedangkan saat menggunakan proxy memiliki rata-rata 51.5 detik yang berarti waktu transfernya 13% lebih cepat dari kondisi normal, dan SSH tunnel dengan waktu transfer hanya 46.83 yang berarti 25% lebih cepat dibandingkan saat menggunakan jaringan Cobralink secara normal.



Gambar 5. Diagram Perbandingan Transfer Time File Gambar

2) Analisis Pengukuran Dengan Data Berupa File Suara

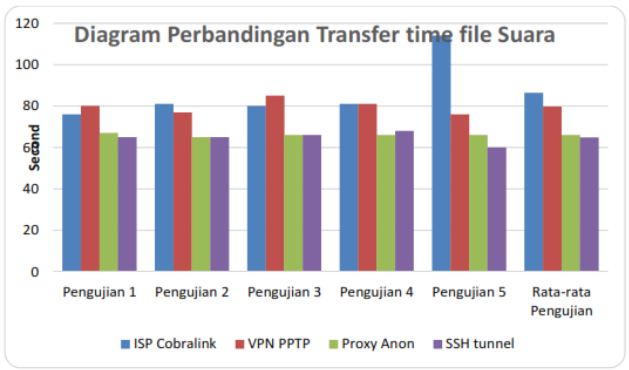
Pada pengukuran ini yaitu berupa file gambar dengan format MPEG Layer 3 (mp3) berukuran 3.12 MB dengan bitrate 320 kbps dari server ke client sebanyak lima kali. Data paket nilai throughput yang digunakan di ambil dari average download pada perintah curl berupa bytes per second sehingga perlu dikalikan 8 untuk memperoleh satuan bit per second.



Gambar 6. Diagram Data Troughput File Suara

Dari Diagram diatas dapat dilihat pada pengujian 1 sampai 5 nilai ketika hanya mengunakan koneksi dari ISP Cobralink memiliki rata-rata throughput 301.0015 Kbit/sec dikarenakan pada pengujian ke 5 mengalami penurunan performa , saat menggunakan VPN PPTP tidak memiliki pengaruh yang signifikan yaitu 319.5078 Kbit/sec yang berarti terjadi kenaikan throughput sebesar 6 % saat menggunakan VPN PPTP, sedangkan saat menggunakan Proxy Anonymous dan SSH Tunnel throughput mengalami kenaikan. Pada proxy Anonymous throughput menjadi 360.4968 Kbit/sec yang berarti mengalami kenaikan yang signifikan sebesar 28 % dibandingkan dengan kondisi normal internet Cobralink dan SSH tunnel mengalami kenaikan yang sama seperti pada penggunaan proxy yaitu yaitu 28% pada throughput rata-rata 398.7796 Kbit/sec lebih cepat dibandingkan saat menggunakan jaringan Cobralink secara normal.

Begitu juga untuk waktu transfernya, dari 5 kali pengujian didapatkan rata ketika menggunakan VPN PPTP 8 % lebih cepat dibandingkan dengan jaringan ISP Cobralink yaitu 79.8 detik sedangkan jaringan ISP Cobralink 86.4 detik, sedangkan saat menggunakan proxy memiliki rata-rata 66 detik yang berarti waktu transfernya 30 % lebih cepat dari kondisi normal, dan SSH tunnel dengan waktu transfer hanya 64.8 yang berarti 33 % lebih cepat dibandingakan saat menggunakan jaringan Cobralink secara normal.



Gambar 7. Diagram Perbandinga Transfer Time File Suara

b. Pengujian Keamanan

Setelah dilakukan pengujian keamanan terhadap ISP Cobralink dan Internet Sharing menggunakan metode serangan *Sniffing to Eavesdrop* dan *Man in the Middle Attack (MITM)* pada 4 keadaan seperti Normal, VPN PPTP, Proxy Anonymous dan SSH Tunnel, maka didapat laporan hasil simulasi uji keamanan seperti pada Gambar berikut:

Metode	ISP Cobralink		Internet Sharing	
	Sniffing to Eavesdrop	*Man in the Middle Attack*	*Sniffing* to Eavesdrop	*Man in the Middle Attack*
Normal	Gagal	Gagal	Berhasil	Berhasil
VPN PPTP	Gagal	Gagal	Gagal	Gagal
Proxy *Anonymous*	Gagal	Gagal	Berhasil	Berhasil
SSH Tunnel	Gagal	Gagal	Gagal	Gagal

Gambar 8. Laporan Hasil Simulasi Uji Keamanan Pada Jaringan

Pada gamar 8 diatas menunjukan bahwa serangan apapun yang penulis lakukan pada jaringan ISP Cobralink tidak membuahkan hasil yang diinginkan, hal tersebut membuktikan bahwa jaringan yang menggunakan Radius server dengan otentikasi Captive Portal yang diterapkan pada ISP Cobarlink sebagai keamanan jaringan WAN dapat mencegah user yang tidak memiliki hak untuk bergabung ke dalam jaringan. Adapun alasan mengapa semua serangan Sniffing to Eavesdrop dan Man in the Middle Attack gagal terjadi pada jaringan yang menggunakan RADIUS server dengan otentifikasi Captive Portal adalah Cara kerjanya yang berbeda dengan enkripsi lainya seperti WEP, WPA, dan WPA2, dimana captive portal menggunakan sistem remote yang harus melalui 3 metode yaitu AAA untuk bisa terhubung ke internet, jadi sebelum user terhubung ke jaringan eksternal, user akan

melewati autentifikasi pada jaringan internal RADIUS terlebih dahulu.

5. PENUTUP

Bedasarkan hasil analisa dan pebandingan yang telah dilakukan dari penelitian pada ISP Cobralink Minomartani, VPN PPTP, Proxy, dan SSH Tunnel, dapat diambil kesimpulan bahwa :

a. Bedasarkan parameter *throughput* pada file gambar, VPN PPTP memiliki nilai *throughput* lebih besar 1.2 % dari ISP Cobralink; Proxy *Anonymous* lebih besar 11 % lebih besar dari ISP Cobralink; sedangkan SSH tunnel lebih besar 23% dari pada saat menggunakan ISP Cobralink.
b. Bedasarkan parameter *throughput* pada file suara, VPN PPTP memiliki nilai *throughput* lebih besar 6 % dari ISP Cobralink; Proxy *Anonymous* lebih besar 28 % lebih besar dari ISP Cobralink; sedangkan SSH tunnel lebih besar 28% dari pada saat menggunakan ISP Cobralink.
c. Bedasarkan parameter *transfer time* pada file gambar, VPN PPTP memiliki nilai *throughput* lebih cepat 2 % dari ISP Cobralink; Proxy *Anonymous* lebih cepat 13 % dari ISP Cobralink; sedangkan SSH tunnel lebih cepat 25% dari pada saat menggunakan ISP Cobralink.
d. Bedasarkan parameter *transfer time* pada file suara, VPN PPTP memiliki nilai *throughput* lebih cepat 8 % dari ISP Cobralink; Proxy *Anonymous* lebih cepat 30 % dari ISP Cobralink; sedangkan SSH tunnel lebih cepat 33% dari pada saat menggunakan ISP Cobralink.
e. Sistem keamanan RADIUS *server* dengan captive portal pada ISP Cobralink membuktikan bahawa memiliki keamanan pada jaringan WAN yang kuat dan juga manajemen user yang terkontrol. Dari hasil pengujian menunjukan bahwa sistem ini sangat sulit untuk ditembus menggunakan teknik ARP *Spoofing* dan *sniffing to eavesdrop.*

6. DAFTAR PUSTAKA

Ariyus, Dony. 2008. Pengantar Ilmu Kripografi Teori. Analisi, dan Implementasi.Andi Yogyakarta.

Thomas,Tom. 2005. Network Security First-Step Yogyakarta. Andi Yogyakarta.

Reza Zurlkanaen.2013. Modul III Virtual Private Network,https://www.academia.edu/6880054/MODUL_III_VIRTUAL_PRIVATE_ NETWORK. di akses pada tanggal 15 Desember 2015

Risanuri.2013.Proxy,http://www.te.ugm.ac.id/~risanuri/jarkom/proxy.doc di akses pada tanggal 15 Januari 2016.

IlmuHacking.2014. Kumpas Tunntas SSH tunneling, http://www.ilmuhacking.com/how-to/kupas-tuntas-ssh-tunneling/ di akses pada tanggal 26 Januari 2016