ANALISIS IMPLEMENTASI KEAMANAN JARINGAN VIRTUAL PRIVATE NETWORK (VPN) PADA PT. LAYAR SENTOSA SHIPPING CORPORATION

Hari Ratmoko[1], Bowo Nurhadiyono[2]
[1,2] Jurusan Desain Komunikasi Visual, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Nakula 5 - 11, Semarang, 50131, 024-3517261
E-mail : hari@larsen.co.id[1], masowo68@gmail.com[2]

Abstrak

Pada awal berdirinya, PT Layar Sentosa Shipping Corp. melakukan transaksi yang dikirimkan dalam bentuk e-mail melalui media internet tanpa pengamanan apapun, hingga pada suatu ketika ada e-mail yang dapat dibaca oleh pihak yang tidak berkepentingan. Oleh karena itu, sejak Januari 2012 yang lalu, perusahaan ini memutuskan untuk menggunakan metode Virtual Private Network (VPN) untuk mengamankan lalu-lintas data dan e-mail tersebut. Dalam penelitian ini, dilakukan pengujian terhadap implementai VPN tersebut. Pengujian-pengujian yang dilakukan adalah pengujian terhadap konektivitas jaringan dengan parameter packet loss, round trip time dan transfer file melalui FTP. Selanjutnya, dilakukan pengujian terhadap tingkat keamanan VPN dengan melakukan serangan (attacking) dengan metode Denial of Service (Dos), Man-in-the-Middle (MITM) dengan aplikasi sniffer dan hacking dengan aplikasi Linux Bactrack. Hasil ekperimen pengujian konektivitas memberikan kesimpulan bahwa bandwidth merupakan faktor utama yang menentukan baik-buruknya konektivitas jaringan antar kantor. Pada eksperimen pengujian keamanan VPN, serangan (attacking) dengan Denial of Service (DoS) ternyata berhasil mematikan service atau layanan pada server VPN. Selain itu, pengujian penyadapan (spoofing) berhasil membaca komunikasi data antara client dengan server VPN. Dan yang terakhir, hacking untuk mendapatkan username dan password dengan menggunakan tools yang ada pada aplikasi Linux Backtrack juga berhasil menembus akses login client ke server VPN.

Kata Kunci: *vpn, konektivitas, attacking, spoofing, hacking.*

1. PENDAHULUAN

1.1. Latar Belakang

Kemajuan di bidang teknologi informasi khususnya *internet* benar-benar berdampak pada aktifitas di dalam sebuah perusahaan, instansi dan bentuk usaha lainnya dalam berinteraksi dengan kantor cabang, karyawan di lapangan maupun konsumen melalui jaringan komputer. Aktifitas-aktifitas tersebut tentu saja dapat beresiko apabila informasi yang penting dan berharga diakses oleh pihak yang tidak berkepentingan.

PT Layar Sentosa *Shipping* Corp. yang bergerak di bidang jasa pengiriman laut (*Shipping Line*), dalam pengiriman data berupa data keuangan, data kepegawaian, data *program update* terbaru, data penawaran harga kepada eksportir dan importir, data transaksi dengan eksportir dan importir, maupun data-data lainnya antara kantor pusat di Jakarta dengan kantor-kantor cabang yang berada di Semarang, Surabaya, dan Bandung dilakukan secara *online*.

Sejak awal berdirinya perusahaan di tahun 2000, PT Layar Sentosa *Shipping*

Corp. menggunakan *e-mail* untuk pengiriman data-data perusahaan. Awalnya semua berjalan lancar tanpa gangguan berarti, hingga pada suatu ketika terjadi masalah yaitu *e-mail* yang dikirim berhasil diacak-acak atau diganggu oleh orang yang tidak berkepentingan karena orang tersebut mengetahui *password* dari alamat *e-mail* penerima. Hal ini mengakibatkan bocornya data-data penting perusahaan yang dikirim tersebut.

Perusahaan menyadari bahwa keamanan data merupakan hal yang sangat penting dan mendasar serta menjadi salah satu faktor penentu kemajuan perusahaan. Oleh karena itu, pengiriman dan penerimaan data membutuhkan suatu metode yang memiliki tingkat keamanan tinggi namun tetap ekonomis. Atas dasar pertimbangan teknis dan komersial itulah, perusahaan akhirnya memutuskan untuk mengimplementasikan metode *Virtual Private Network* (VPN) sejak Januari 2012.

1.2. Rumusan Masalah

Dari latar belakang yang dijelaskan di atas, ditemukan beberapa masalah yang dirumuskan ke dalam suatu rumusan masalah, yaitu:

1. Bagaimana mengetahui efektifitas dari *Virtual Private Number* (VPN) yang saat ini digunakan.
2. Bagaimana mengetahui bahwa *Virtual Private Number* (VPN) yang saat ini digunakan benar-benar sudah menjamin keamanan data dari gangguan pihak luar.

1.3. Batasan Masalah

Dalam penelitian dan Tugas Akhir ini, hanya dibatasi pada pengujian terhadap:

1. Konektivitas jaringan dengan menggunakan parameter:
    a. *Packet Loss*,
    b. *Round Trip,* dan
    c. *FTP Transfer*.
2. Keamanan transfer data dengan melakukan serangan (*attacking*) terhadap VPN menggunakan:
    a. Metode *Denial of Services* (DoS),
    b. Aplikasi atau *software Man-In-The-Middle-Attack* (MIMA), dan
    c. Aplikasi atau *software Hacking VPN* dengan melakukan *ARP Poisoning* di *Linux Backtrack*.

1.4. Tujuan Penelitian

Tujuan dari penelitian dan Tugas Akhir ini adalah untuk:

1. Mengetahui performa dari konektivitas jaringan *Virtual Private Number* (VPN) di PT Layar Sentosa Shipping Corp.
2. Mengetahui tingkat keamanan jaringan *Virtual Private Number* (VPN) di PT Layar Sentosa Shipping Corp.

1.5. Manfaat Penelitian

Manfaat dari penelitian dan Tugas Akhir ini adalah sebagai berikut:

1. Bagi penulis: memperkaya pengetahuan dan memperdalam pemahaman tentang metode *Virtual Private Network* (VPN).
2. Bagi perusahaan: mengetahui lebih jauh tingkat efektivitas, efisiensi dan keamanan komunikasi data di *internet* dengan menggunakan metode *Virtual Private Network* (VPN) baik ditinjau dari segi teknis maupun komersial.
3. Bagi mahasiswa: sebagai referensi dalam penelitian lain yang berkaitan dengan *Virtual Private Network* (VPN).

1.6. Rencana Pemecahan Masalah

1. Solusi untuk mengatasi permasalahan kelemahan jaringan di PT. Layar Sentosa Shipping adalah dengan meningkatkan pengamanan di level *server* dan *gateway/router*-nya dengan memasang aplikasi *anti flooding*.
2. Perlunya pembenahan pada *security* jaringan dan manajemen *password*-nya. Solusinya sementar adalah dengan cara dibuat dengan kombinasi huruf dan angka serta *password*-nya dibuat lebih dari 10 digit dan terdiri dari kombinasi huruf dan angka. Hal ini bertujuan untuk menyulitkan aksi *generate key* oleh *attacker* (penyerang).
3. Perlunya merubah kebiasaan *user* yang suka menggunakan *username* dan *password* dengan jumlah digit pendek, karena hal ini rentan terhadap penyadapan oleh orang yang tidak berhak (MITM).

1.7. Tinjauan Pustaka

1. Chou. 2008, *Strong User Authentication on the Web. United State: Microsoft Corporation.*
2. Frankel S. et. al. 2005. *Guide to IPSec VPN.National Institute of Standards and Technology*. Departemen Komersial Amerika Serikat.
3. Madjid. N. 2010, *Perbandingan Ssl (Secure Socket Layer)Dan Ipsec (Internet Protocol Security) Pada Vpn (Virtual Private Network).* Surabaya: *Electrical Engineering Polytechnic Institute of Surabaya* (EEPIS).
4. Sari M.W. 2011, Analisis Keamanan Jaringan Virtual Private Network (VPN) pada Sistem Online Microbanking (Kasus di BMT Al Ikhlas Yogyakarta). Universitas Gadjah Mada. Yogyakarta.
5. Sukaridhoto.S. 2005. *Teknik Keamanan Pada Voip Dengan Virtual Private Networking Dan Kriptografi Serta Korelasi Terhadap Bandwidth Dan Intelligibility Suara,* Surabaya: *Electrical Engineering Polytechnic Institute of Surabaya* (EEPIS).
6. Thomas, Tom. 2005. *Network Security First Step.* Penerbit Andi, Yogyakarta.

6.2. Hipotesis

1. Hasil pengujian konektivitas jaringan VPN:
   a. *Packet Loss*: konektivitas antara kantor Semarang dan kantor pusat Jakarta lebih baik (dengan tingkat *packet loss* 4%) daripada konektivitas antara kantor Semarang dan kantor Surabaya (dengan tingkat *packet loss* 5%).

b. *Round Trip Time*: *round trip time* dari kantor Semarang ke kantor Jakarta lebih singkat (RTT: 24 *millisecond*) daripada *round trip time* dari kantor Semarang ke kantor Surabaya (RTT: 42 *millisecond*).
c. FTP *Transfer*: semakin besar *bandwidth* maka proses transfer *file* juga akan semakin cepat. Selain itu, penulis sangat menyayangkan karena selama ini fasilitas FTP *server* tidak diaktifkan. Padahal dari sisi keamanan, fasilitas ini bisa diamankan dengan *login username* dan *password*.

2. Hasil pengujian keamanan jaringan VPN:
   a. *Denial of Service* (DoS) dengan *pingflood attack*: berhasil menyerang dan mengganggu aktivitas jaringan di *server* VPN PT Layar Sentosa Shipping Corp.
   b. *Man-In-the-Middle* (MITM) *Attack*: *attacker* (penyerang) berhasil melakukan *spoofing* terhadap komputer *client* dengan IP *address*: 10.252.108.208 yang sedang bertukar data dengan *server* dengan IP *address*: 10.252.108.127. Hal ini terbukti dari berubahnya MAC Number *client* dari 00:00:e2:9b:3c:b8 menjadi 00:e0:7d:dd:50:0e dan MAC Number *server* dari 00:e0:7d:dd:50:0f menjadi 00:e0:7d:dd:50:0e.
   c. *Hacking* Menggunakan *Linux Bactrack*: *attacker* (penyerang) berhasil membaca *username* dan *password* VPN dari salah satu komputer *client*.
3. Evaluasi Jaringan VPN dan Non-VPN menunjukkan hasil bahwa aktifitas di jaringan VPN lebih baik daripada Non-VPN karena aktivitas yang dilakukan di dalam *tunnel* VPN tidak diketahui oleh orang lain.
4. Kriptografi yang digunakan PT Layar Sentosa Shipping Corp. adalah CISCO *Guard* XT & CISCO *Traffic Anomaly Detector* XT yang merupakan paket layanan yang diberikan oleh PT Indosat Tbk sebagai operator telekomunikasi. CISCO *Guard* XT & CISCO *Traffic Anomaly Detector* XT mampu mendeteksi serangan DoS, DDoS, worm dan jenis serangan lainnya dengan cara memblokir lalu-lintas serangan dan mencegah setiap jenis serangan terhadap jaringan komputer. Ketika CISCO *Traffic Anomaly Detector* XT mengidentifikasi potensi serangan, ia akan menginformasikannya kepada CISCO Guard XT untuk mulai mengalihkan lalu-lintas data yang menjadi target serangan tersebut.

2. METODE

3.1. Jenis Data

Dalam penelitian ini, penulis menggunakan data penelitian kuantitatif, karena data yang diperoloeh nantinya berupa angka. Dari angka yang diperoleh akan dianalisis lebih lanjut dalam analisis data.

3.2. Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan dalam penelitian ini adalah:

3.2.1. Studi Literatur

Studi literatur dilakukan untuk mencari dan mempelajari sumber-sumber informasi dari beberapa artikel & jurnal ilmiah yang berkaitan dengan jaringan *Virtual Private Network* (VPN) dan beberapa jenis serangan terhadap jaringan

VPN tersebut. Tahap ini sangat penting dalam rangka membangun pemahaman yang benar sebelum melalukan pengujian.

3.2.2. Wawancara

Wawancara dilakukan kepada IT *Officer* yang sejak awal diberi tanggung-jawab untuk melakukan migrasi dari jaringan lama ke jaringan *Virtual Private Network* (VPN). IT *Officer* ini juga bertanggung-jawab atas keamanan jaringan dan data sejak diimplementasikan pada Januari 2012 yang lalu.

3.2.3. Eksperimen Pengujian

Pada tahap ini, dilakukan beberapa pengujian terhadap jaringan *Virtual Private Network* (VPN), yaitu pada stabilitas koneksi jaringan VPN dan pengujian pada keamanan jaringan VPN. Langkah-langkah pengujiannya adalah sebagai berikut:

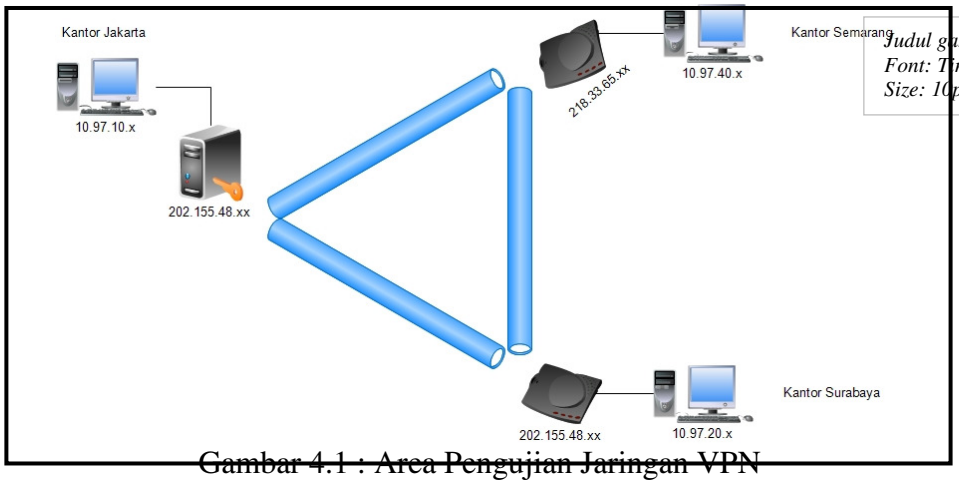
1. Oberservasi. Oberservasi dilakukan terhadap semua komputer client yang seluruhnya berjumlah 12 client, 1 buah router dan 1 buah server.
2. Persiapan hardware berupa 1 buah komputer *client* (di luar 12 komputer *client* yang sudah ada) yang akan digunakan khusus untuk melakukan serangan (*attacking*) terhadap jaringan VPN perusahaan.
3. Instalasi aplikasi serangan (*attacking*) yaitu *Denial of Service* (DoS) dan *Man-in-the-Middle* (MITM) serta aplikasi *hacking* yaitu *Linux Backtrack*. Aplikasi-aplikasi tersebut di atas di-*install* ke dalam komputer *client* yang khusus sebagaimana disebutkan dalam poin 2.
4. Pengujian konektivitas dengan menggunakan parameter:
    a. *Packet Loss*: pengujian ini digunakan untuk memantau rata-rata, minimum dan maksimum packet loss yang melalui *tunnel* VPN.
    b. *Roud Trip Time*: pengujian ini digunakan untuk menghitung rata-rata dan maksimum waktu round trip pada *tunnel* yang ada dengan menggunakan *ping*.
    c. Transfer file *melalui FTP*: pengujian ini dilakukan untuk mengetahui waktu yang dibutuhan untuk trasfer file melalui *tunnel* VPN.
5. Pengujian terhadap keamanan jaringan VPN dengan melakukan *attacking* dan *hacking*, yaitu:
    a. *Attacking* dengan metode *Denial of Services* (DoS): melakukan serangan ping dengan aplikasi pingflood.exe, dimana IP address target yang akan diserang adalah IP public pada *server* VPN.
    b. *Attacking* bertindak sebagai *Man-In-The-Middle* (MITM) dengan menjalankan program *sniffer*: melakukan penyadapan terhadap komunikasi antara *server* dengan komputer *client* di kantor Semarang.
    c. *Hacking* dengan menggunakan aplikasi atau *software Linux Backtrack*: melakukan hacking terhadap salah satu komputer *client* di Divisi Marketing.

6. Analisis terhadap hasil pengujian konektivitas dengan menggunakan parameter:
   a. *Packet Loss*: konektivitas dari kantor Semarang ke kantor pusat Jakarta (packet loss 4%) lebih baik daripada konektivitas ke kantor Surabaya (packet loss 5%).
   b. *Roud Trip Time*: round trip time dari kantor Semarang ke kantor Jakarta lebih singkat daripada round trip time ke kantor Surabaya.
   c. Transfer file *melalui FTP*: semakin besar bandwidth maka proses transfer file juga akan semakin cepat.
7. Analisis terhadap hasil pengujian terhadap keamanan jaringan VPN dengan melakukan *attacking* dan *hacking*, yaitu:
   a. *Attacking* dengan metode *Denial of Services* (DoS): *pingflood* berhasil menyerang dan mengganggu aktivitas jaringan di *server* VPN PT Layar Sentosa Shipping Corp.
   b. *Attacking* bertindak sebagai *Man-In-The-Middle* (MITM) dengan menjalankan program *sniffer*: *attacker* berhasil melakukan *spoofing* terhadap komputer *client* yang sedang bertukar data dengan *server*.
   c. *Hacking* dengan menggunakan aplikasi atau *software Linux Backtrack*: *username* & *password* bisa ditembus/di-*hack*.

3. HASIL DAN PEMBAHASAN

1.1.Eksperimen *Network Setup* dan Tes Kondisi

Tes kondisi dilakukan dengan cara *trace route* langsung ke IP *virtual*, hasilnya adalah 10.97.40.x (IP virtual Semarang), 10.97.10.x (IP virtual Jakarta) dan 10.97.20.x (IP virtual Surabaya). Area jaringan yang dilakukan pengujian adalah VPN kantor pusat di Jakarta, kantor cabang di Semarang, dan kantor cabang di Surabaya. Gambar 4.1 menunjukkan area pengujian jaringan VPN.



Gambar 4.1 : Area Pengujian Jaringan VPN

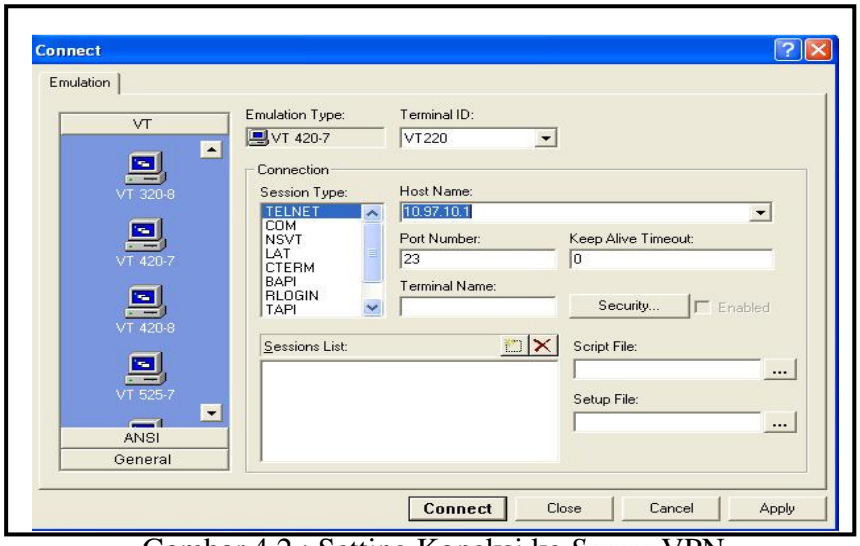
1.2. Uji Konektivitas Jaringan

Uji konektivitas yang dilakukan melalui kantor pusat di Jakarta dengan kantor

cabang di Bandung dan kantor cabang di Surabaya pada tanggal 31 Maret 2014 pada pukul 13:00 WIB sampai dengan pukul 16:00 WIB menggunakan konfigurasi alamat IP sebagai berikut:

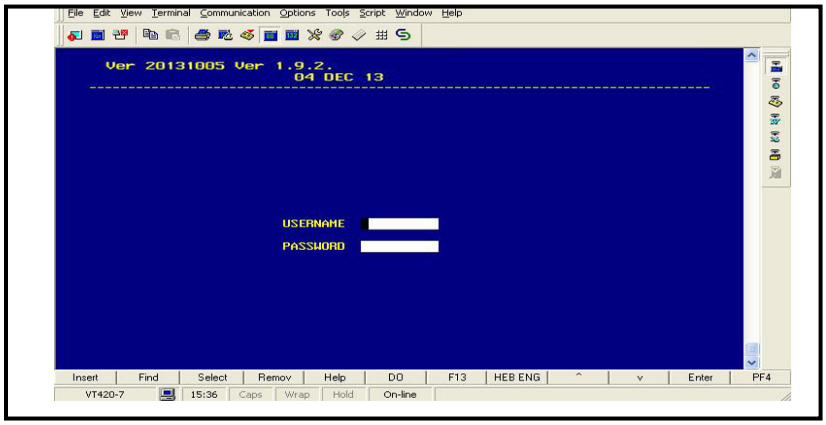
1. IP public PT Layar Sentosa Shipping di Jakarta:
    - IP: 202.155.xx.xx
    - Subnet Mask: 255.255.255.252
    - Default Gateway:
2. IP kantor cabang di Semarang:
    - IP: 218.33.xx.xx
    - Subnet Mask: 255.255.255.252
    - Default Gateway:
3. IP kantor cabang di Surabaya:
    - IP: 202.155.xx.xx
    - Subnet Mask: 255.255.255.224
    - Default Gateway:

Eksperimen uji konektivitas diawali terlebih dahulu dengan menjalankan *software VPN client*. Setelah itu, muncul tampilan masukkan nama komputer *server* VPN dan IP *public*-nya. Lalu, *connect* untuk masuk atau tombol *exit* untuk keluar. Tampilannya dapat dilihat pada Gambar 4.2.



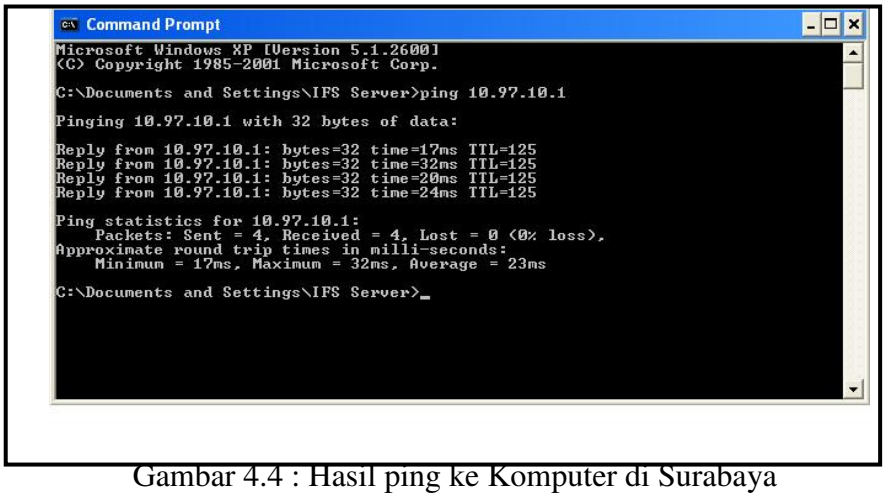
Gambar 4.2 : Setting Koneksi ke *Server* VPN

Setelah terhubung ke *server*, selanjutnya muncul tampilan *login user*, hanya *user* yang terdaftar saja yang bisa menggunakan fasilitas jaringan VPN. Tampilannya ditunjukkan pada Gambar 4.3.



Gambar 4.3 : Tampilan Login User VPN

Uji konektivitas dilakukan dengan cara ping dari komputer kantor pusat di Jakarta ke komputer kantor cabang di Surabaya, ditunjukkan pada Gambar 4:4.



Gambar 4.4 : Hasil ping ke Komputer di Surabaya

1.3. Mekanisme Pengujian Konektivitas

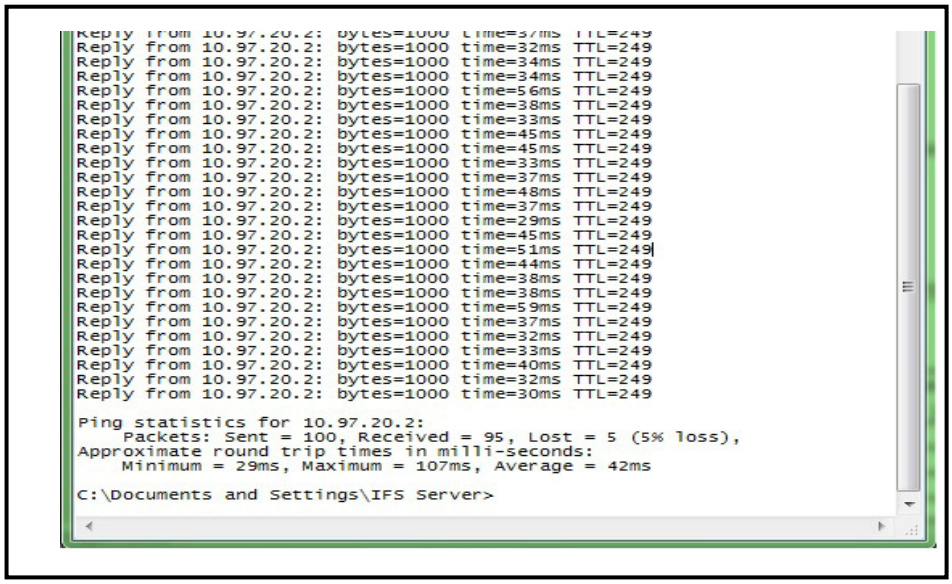
Mekanisme pengujian konektivitas pada penelitian ini dilakukan dengan beberapa parameter, yaitu:

1. *Packet Loss,*
2. *Round Trip,* dan
3. *FTP Transfer.*

Berikut ini penjelasan parameter pengujian konektivitas:

1. *Packet Loss*

   Eksperimen pengujian ini digunakan untuk memantau rata-rata, minimum dan maksimum packet loss yang melalui *tunnel* VPN. Di setiap lokasi pengujian dilakukan pengiriman 1000 bytes data dengan 100 kali tes sebagaimana ditunjukkan pada Gambar 4.5.



Gambar 4.5 : Pengujian *Packet Loss* dengan Ping

Eksperimen ping ini dilakukan ke *server* data sebagai IP tujuan. Packet loss ini bertujuan untuk mengetahui rata-rata loss/kehilangan dalam 30 kali tes.

Tabel 4.1 : *Packet Loss* pada *tunnel* VPN

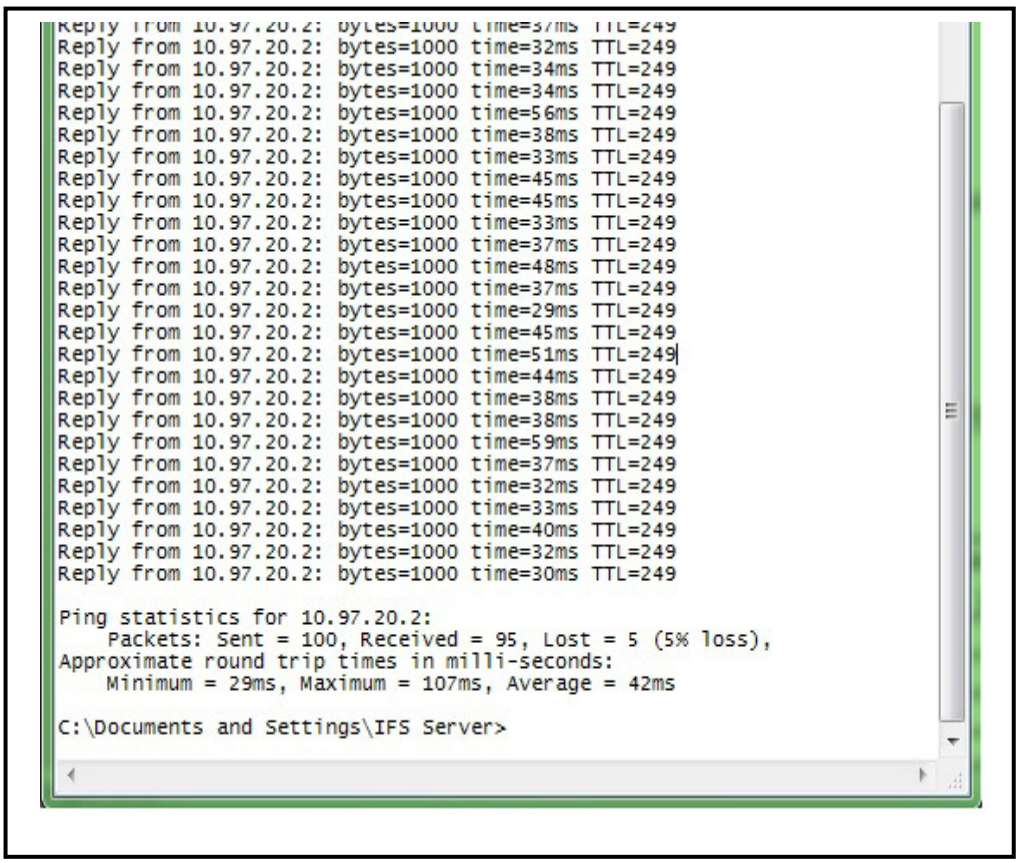
Lokasi Pengujian Kantor Semarang					
Ip Sumber	**Ip Tujuan**	**Bytes**	**Packet**		**Packet Loss (%)**
			Dikirim	**Diterima**	
10.97.40.X	**10.97.10.x**	**1000**	**100**	**96**	**4**
10.97.40.X	**10.97.20.x**	**1000**	**100**	**95**	**5**

Data statistik pada Tabel 4.1 di atas menunjukkan hal-hal sebagai berikut, yaitu:

a. Dari 1000 bytes data yang dikirim dari kantor Semarang (IP sumber: 10.97.40.x) ke kantor pusat Jakarta (IP tujuan: 10.97.10.x), terdapat packet loss sebessar 4%.
b. Dari 1000 bytes data yang dikirim dari kantor Semarang (IP sumber: 10.97.40.x) ke kantor Surabaya (IP tujuan: 10.97.20.x), terdapat packet loss sebesar 5%.
c. Dapat ditarik kesimpulan bahwa konektivitas dari kantor Semarang ke kantor pusat Jakarta (packet loss 4%) lebih baik daripada konektivitas ke kantor Surabaya (packet loss 5%).

2. *Round Trip Time* (RTT)

Eksperimen pengujian round trip digunakan untuk menghitung rata-rata dan maksimum waktu round trip pada tunnel yang ada dengan menggunakan *ping*.



Gambar 4.6 : Pengujian *Round Trip Time* dengan *Ping*

Hasil dari eksperimen ini sama dengan hasil *packet loss* karena *packet loss* dan *round trip time* merupakan satu-kesatuan tes pada perintah ping. Karena ping bertujuan untuk menghitung waktu statistik *round trip time* dan *packet loss*. *Round Trip Time* adalah perjalanan paket *ping* dari komputer yang digunakan untuk melakukan *ping*, kemudian ke *host router* data kembali lagi ke komputer *client*, atau secara sederhana diartikan sebagai perjalanan pulang pergi.

Tabel 4.2 : *Round Trip Time* pada *Tunnel* VPN

Lokasi Pengujian Kantor Semarang					
IP Sumber	**IP Tujuan**	**Bytes**	**RTT Packet dalam Milisecond**		**RTT Packet dalam Millisecond**
			Min.	**Max.**	
10.97.40.x	**10.97.10.x**	**1000**	**14**	**100**	**24**
10.97.40.x	**10.97.20.x**	**1000**	**29**	**107**	**42**

Data statistik pada Tabel 4.2 di atas menunjukkan hal-hal sebagai berikut, yaitu:

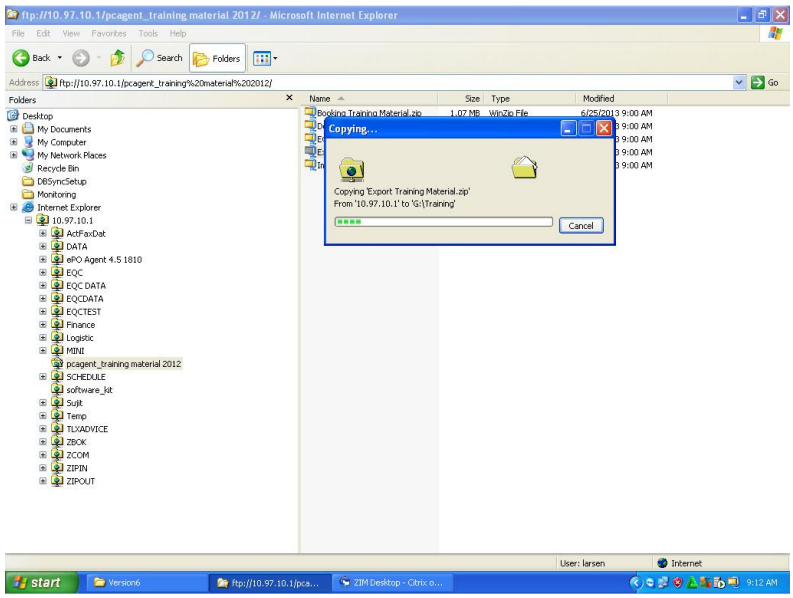
a. Dari kantor Semarang (IP sumber: 10.97.40.x) ke kantor pusat Jakarta (IP tujuan: 10.97.10.x), round trip time minimim dari 1000 bytes data yang dikirim adalah 14 millisecond dan round trip maximumnya adalah 100 millisecond, dengan rata-rata round trip time 24 millisecond.
b. Dari kantor Semarang (IP sumber: 10.97.40.x) ke kantor Surabaya (IP tujuan: 10.97.20.x), round trip time minimim dari 1000 bytes data yang dikirim adalah 29 millisecond dan round trip maximumnya adalah 107 millisecond, dengan rata-rata round trip time 42 millisecond.
c. Dari data-data statistik tersebut di atas, dapat diambil kesimpulan bahwa *round trip time* dari kantor Semarang ke kantor Jakarta lebih singkat daripada *round trip time* ke kantor Surabaya.

3. Transfer File *melalui FTP*

Eksperimen pengujian ini diharapkan bisa mengetahui waktu yang dibutuhan untuk trasfer file melalui tunnel VPN, walaupun fasilitas FTP *server* selama ini tidak diaktifkan di komputer *server* data, karena alasan keamanan data perusahaan supaya tidak bocor kepada orang yang tidak berkepentingan. Tetapi, untuk uji kecepatan download file melalui FTP *server* untuk sementara waktu dilakukan dengan melakukan pengaturan *user name* dan *password* demi keamanan. Hal ini ditunjukkan pada Gambar 4.7.

Gambar 4.7 : Tampilan user login ke FTP *Server*

Dalam eksperimen ini, file yang di-*download* adalah file *Export Training Material.zip* yang berukuran 1,08 MB, yang ditunjukkan pada Gambar 4.8.



Gambar 4.8 : Download File via FTP

Berikut hasil eksperimen download/transfer file, waktu yang dibutuhkan dalam proses *download* mulai dari awal proses simpan berkas sampai proses *download*-nya berakhir dihitung menggunakan stopwatch, dan untuk eksperimen ini dilakukan hanya 1 kali tes download di masing-masing lokasi pengujian. Hasilnya ditunjukkan pada Tabel 4.3.

Tabel 4.3 : File Transfer via FTP pada *Tunnel* VPN

Lokasi Pengujian	IP Sumber	IP Tujuan	Bandwidth	Waktu Transmisi
Kantor Jakarta	**10.97.10.x**	**10.97.10.x**	**3 Mbps**	**00:26:03:51**
Kantor Semarang	**10.97.40.x**	**10.97.10.x**	**2 Mbps**	**00:30:09:52**
Kantor Surabaya	**10.97.20.x**	**10.97.10.x**	**1 Mbps**	**00:52:21:33**

Data statistik pada Tabel 4.2 di atas menunjukkan hal-hal sebagai berikut, yaitu:

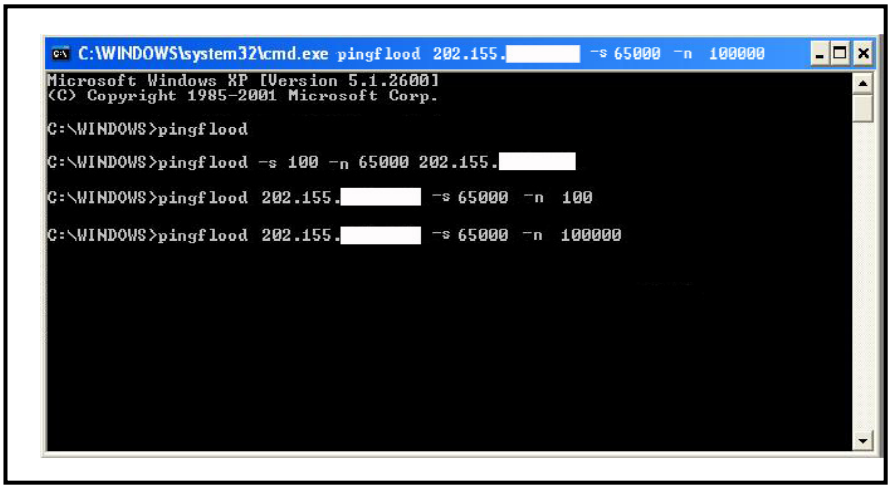
a. Di kantor pusat Jakarta (IP sumber: 10.97.10.x ke IP tujuan 10.97.40.x), file transfer melalui FTP memerlukan waktu: 26 menit, 3 detik dan 51 milidetik.
b. Dari kantor Semarang (IP sumber: 10.97.40.x) ke kantor pusat Jakarta (IP tujuan: 10.97.10.x), file transfer melalui FTP memerlukan waktu: 30 menit, 9 detik dan 52 milidetik.
c. Dari kantor Surabaya (IP sumber: 10.97.20.x) ke kantor pusat Jakarta (IP tujuan: 10.97.10.x), file transfer melalui FTP memerlukan waktu: 52 menit, 21 detik dan 33 milidetik.
d. Dari data-data statistik di atas, dapat ditarik kesimpulan bahwa semakin besar *bandwidth* maka proses transfer *file* juga akan semakin cepat.

1.4. Mekanisme Pengujian Keamanan

Mekanisme pengujian keamanan pada penelitian ini dilakukan dengan beberapa cara atau metode, yaitu:

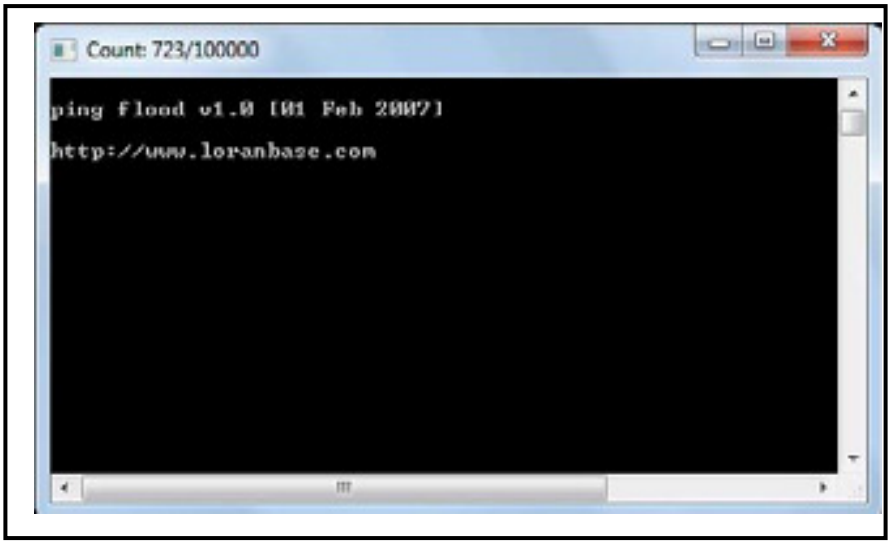
1. *Attacking* Menggunakan *Denial of Service* (DoS)

Pengujian untuk melakukan attack pada komputer *server* dengan menggunakan metode Denial of Service. Eksperimen *Denial of Service* bertujuan untuk menghentikan atau mematikan *service* pada komputer target, dalam hal ini adalah *server* VPN. *Denial of Service* (DoS) dengan aplikasi *pingflood.exe*, IP *address* target yang akan diserang adalah *public* IP *server* VPN (202.155.xx.xx). – *Command prompt* diaktifkan dengan start > run > cmd. Langkah selanjutnya dilakukan dengan perintah: *pingflood* 202.155.xx.xx –s 65000 –n 100000, sebagaimana gambar 4.9.



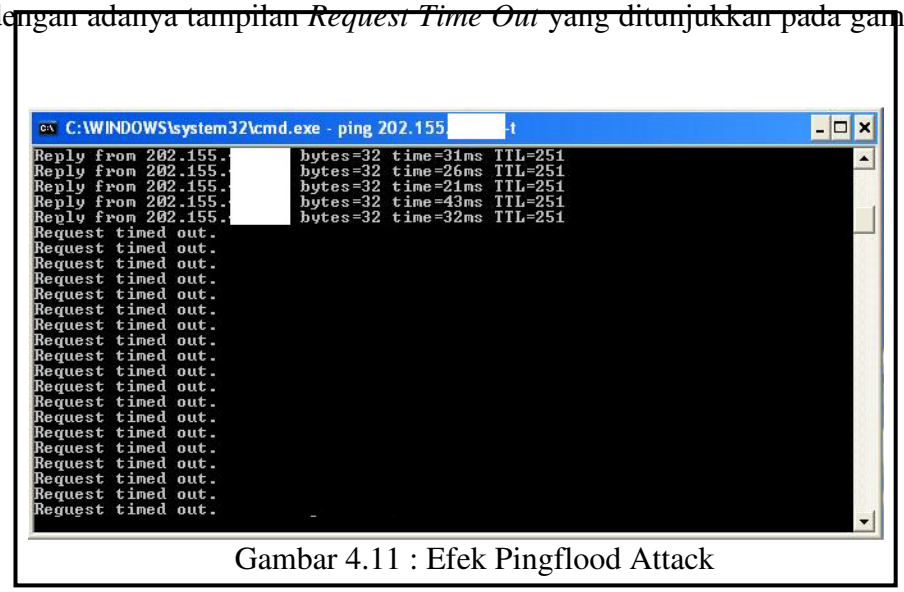
Gambar 4.9 : Perintah *Pingflood*

Gambar 13 menunjukkan perintah *pingflood* yang diarahkan pada IP target, selanjutnya muncul tampilan indikator proses *pingflood* yang ditunjukkan pada Gambar 4:10.



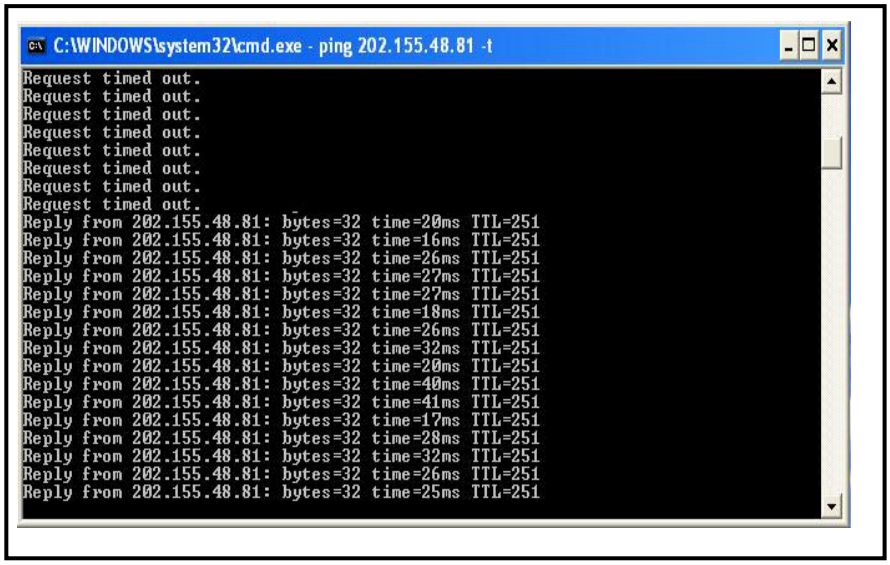
Gambar 4.10 : Indikator Proses *Pingflood*

Gambar 4.10 menunjukkan proses *counter* yang telah mencapai 723 paket dari total 100000 paket yang dikirimkan melalui perintah *pingflood*. Efek dari attack dengan *pingflood* ini tentu berpengaruh pada koneksi antara client VPN dengan *server* VPN, yang semula koneksinya lancar tiba-tiba mengalami *down* dengan adanya tampilan *Request Time Out* yang ditunjukkan pada gambar 4.11.



Gambar 4.11 : Efek Pingflood Attack

Proses *pingflood* attack akan berhenti setelah jumlah paket *pingflood* yang dikirimkan telah terpenuhi yaitu 100000 paket, maka koneksi ke IP target akan kembali normal. Ditunjukkan pada Gambar 4.12.

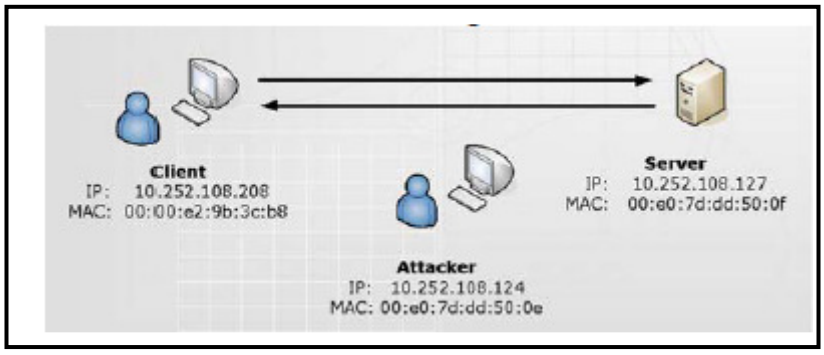


Gambar 4.12 : Akhir dari *Pingflood Attack*

Koneksi IP target normal *Denial of Service* (DoS) a*ttack* dengan menggunakan *pingflood* ternyata memiliki efek yang lebih parah daripada perintah ping biasa. Sehingga dapat disimpulkan bahwa eksperimen *Denial of Service* (DoS) *attack* khususnya *pingflood* ternyata berhasil menyerang dan mengganggu aktivitas jaringan di *server* VPN PT Layar Sentosa Shipping Corp. Hal ini merupakan salah satu kelemahan jaringan di PT Layar Sentosa Shipping Corp. Solusi untuk mengatasi permalsalahan ini adalah dengan meningkatkan pengamanan di level *server* dan *gateway* atau *router*-nya.

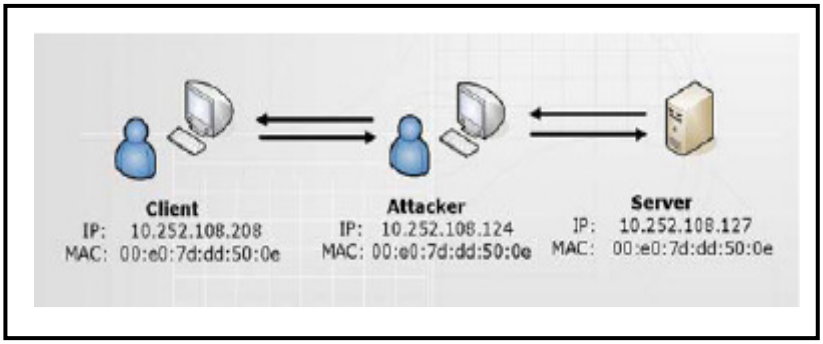
2. *Man-In-the-Middle* (MITM) *Attack*

Untuk dapat membaca atau menyadap dan menganalisa setiap protokol yang melewati mesin, diperlukan sebuah program aplikasi atau *sofware* yang bisa membelokkan paket ke komputer *attacker* (penyerang). Program yang digunakan dalam pengujian ini adalah *sniffer*. Sedangkan akftivitas pembacaan paket disebut *spoofing*.



Gambar 4.13 : Koneksi TCP Sebelum Spoofing

Gambar 4.13 mengilustrasikan koneksi TCP yang sebenarnya, tanpa ada sebuah komputer yang bertindak sebagai MITM. Kemudian komputer *attacker* (penyerang) menjalankan program *sniffer*, berarti komputer *attacker* (penyerang) akan bertindak sebagai komputer yang dilewati oleh paket data antara komputer *client* dan *server*.



Gambar 4.14 : Koneksi TCP Setelah Spoofing

Dari hasil pengujian ini, *attacker* berhasil melakukan *spoofing* terhadap komputer *client* dengan IP *address*: 10.252.108.208 yang sedang bertukar data dengan *server* dengan IP *address*: 10.252.108.127.

3. *Hacking* Menggunakan *Linux Bactrack*

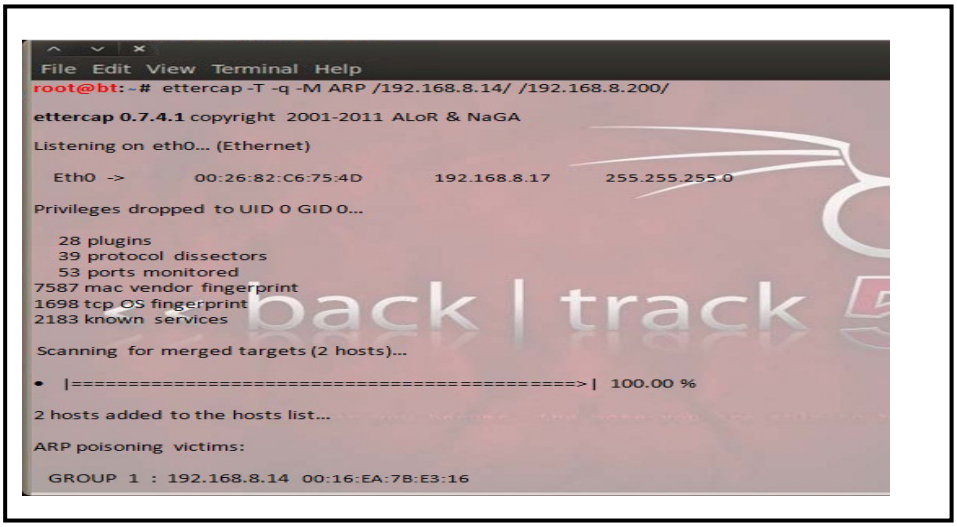
Eksperimen *hacking* menggunakan *Linux Backtrack* bertujuan untuk mendapatkan *username* dan *password* yang digunakan oleh *user* ataupun *client* pada saat koneksi ke *server* VPN. Setting IP *address* jaringan VPN yang akan di-*hack* adalah sebagai berikut:

- IP *server* VPN : 202.155.xx.xx
- Gateway LAN : 192.168.8.200
- IP attacker : 192.168.8.17
- IP client target : 192.168.8.14

Teknik ini biasa dinamakan dengan ARP *Poisoning*. *Tools* yang digunakan adalah *ettercap* yang setara bawaan sudah tersedia di *Linux Backtrack*. *Attacker* menggunakan *ettercap* pada mode text. Contoh sintax-nya adalah: ettercap –T –q –M ARP /ip target/ip gateway/ atau ettercap –T –q –M ARP /192.168.8.14/ / 192.168.8.14/ /192.168.8.200/.

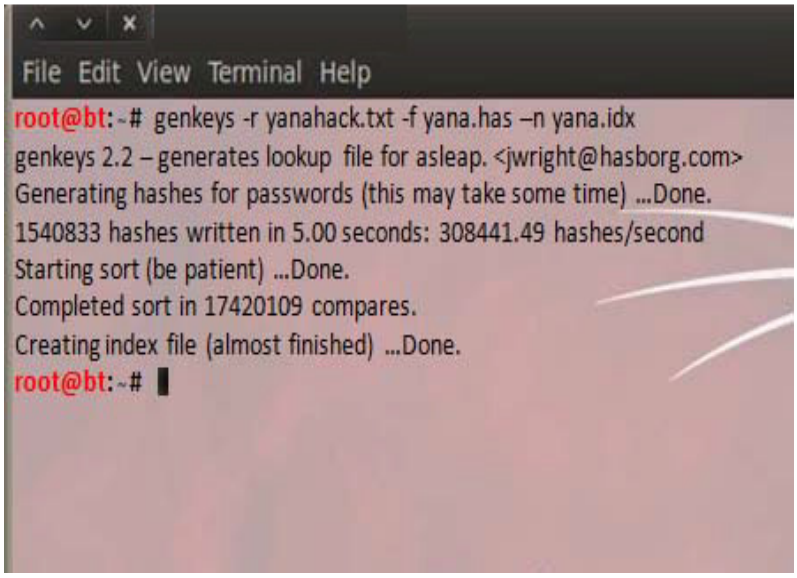
- option –T : mode text
- option –q : ettercap dijalankan dalam keadaan tenang/outputnya tidak terlalu banyak
- option –M : menggunakan teknik ARP

Penerapan ARP Poisoning pada sintax tersebut ditunjukkan pada Gambar 4.15.



Gambar 4.15 : *Sintax Ettercap Hacking* pada *Linux Bactrack*

Sintax *ettercap hacking* pada *Linux Backtrack* ini menggunakan teknik *bruteforce* dengan menggunakan file kamus (wordlist.txtl yanahack.txt) dengan harapan *password* dari komputer target ada di dalam file tersebut. Untuk itu, terlebih dahulu dibuat *file hash* dan *file index* dari *wordlist* yang sudah ada. Program yang digunakan untuk membuat *file hash* dan *index* adalah *genkeys* yang ditunjukkan pada Gambar 4.16.

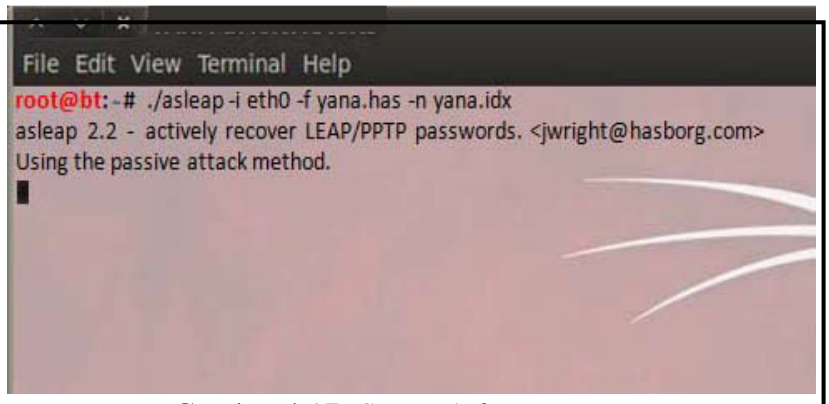


Gambar 4.16 : *Sintax Genkeys*

Gambar 4.16 menunjukkan hasil berupa file yana.hash yana.idx.

- option –r : meminta *input*-an dari sebuah *file* (dalam hal ini *file wordlist*)
- option –f : akan membuat *output* dari *file wordlist* menjadi *file-file hash*
- option –n : akan membuat output berupa *file index* dari *wordlist*

Kedua file baru tersebut dibutuhkan oleh program VPN *crack* yang akan digunakan yaitu *asleap*. Tahap berikutnya adalah *bruteforce* dengan menggunakan *asleap*, tapi yang digunakan adalah *asleap* bawaan dari *Linux Bactrack 5*. Hal ini ditunjukkan pada Gambar 4.17.

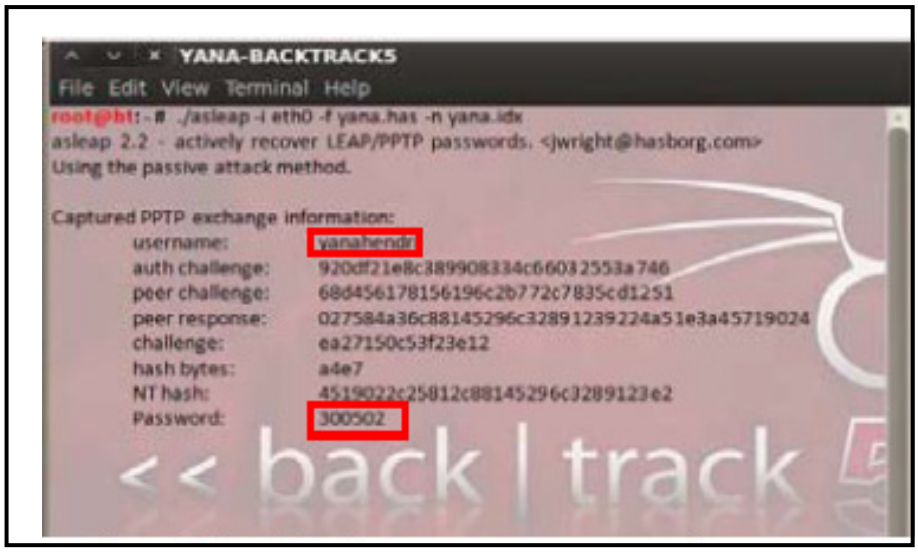


Gambar 4.17: *Sintax Asleap*

Gambar 4.17 menunjukkan adanya beberapa option yang digunakan, yaitu:

- Option –i : menunjukkan *interface/ethernet* yang digunakan, misalnya eth0
- Option –f : meminta inputan dari *file hash* yang sudah dibuat
- Option –n : meminta inputan dari *file index* yang sudah dibuat

Ketika target melalukan koneksi ke *server* VPN, maka bisa dilihat *output capture* koneksi sehingga dapat dilihat *username* dan *password* yang dilakukan oleh *user* komputer target. Hasil *capture*-nya ditunjukkan pada Gambar 4.18 dalam kotak berwarna merah.



Gambar 4.18 : *Capture Username* dan *Password*

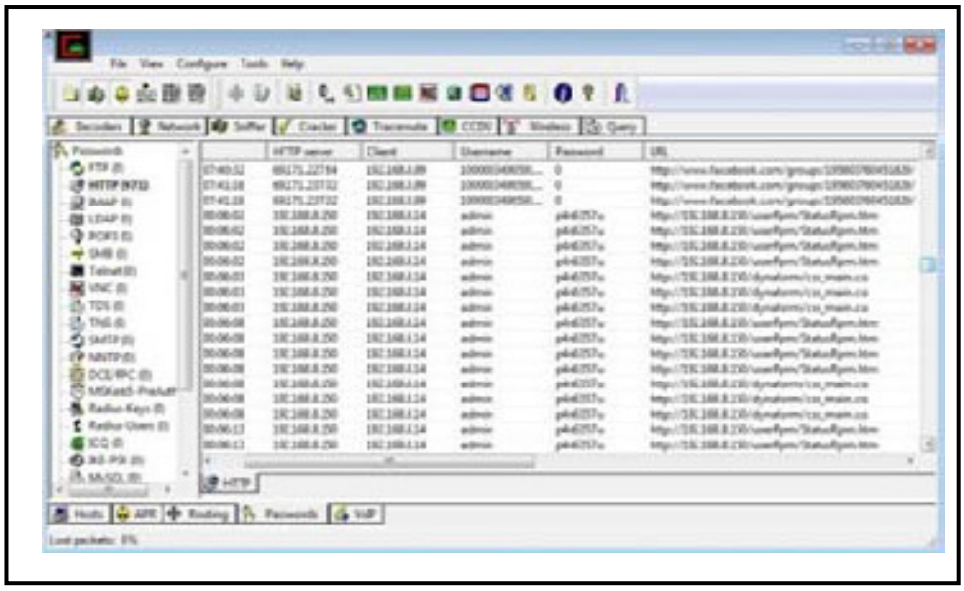
Berdasarkan pengujian *hacking* dengan menggunakan *Linux Bactrack*, maka dapat disimpulkan bahwa keamanan jaringan VPN di PT Layar Sentosa Shipping Corp. masih ada kelemahan karena masih bisa di-*hack* pada *username* & *password*-nya.

1.5. Evaluasi Jaringan Non-VPN

Evaluasi jaringan non-VPN ini dilakukan dengan cara mematikan fasilitas VPN dengan tidak mengaktifkan *server* VPN untuk sementara waktu.

1.5.1. Pengujian Menggunakan *Software Cain & Abel*

Pada eksperimen ini dilakukan percobaan sniffing pada jaringan non-VPN di PT Layar Sentosa Shipping Corp. dengan menggunakan *software Cain & Abel*.

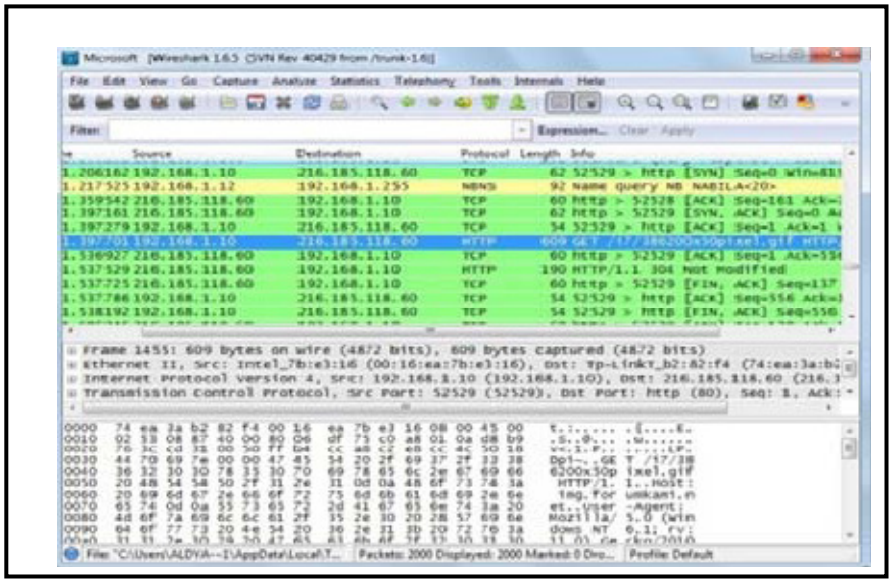


Gambar 4.19 : Cain & Abel pada Jaringan Non-VPN

Gambar 4.19 menunjukkan bahwa ada beberapa penyadapan yang dilakukan pada IP *Access Point* dengan terlihatnya *username* dan *password*.

1.5.2. Pengujian Menggunakan *Software Wireshark*

Pada eksperimen ini dilakukan sniffing pada jaringan non-VPN di PT Layar Sentosa Shipping Corp. dengan menggunakan *software Wireshark*.



Gambar 4.20 : *Wireshark* pada Jaringan Non-VPN

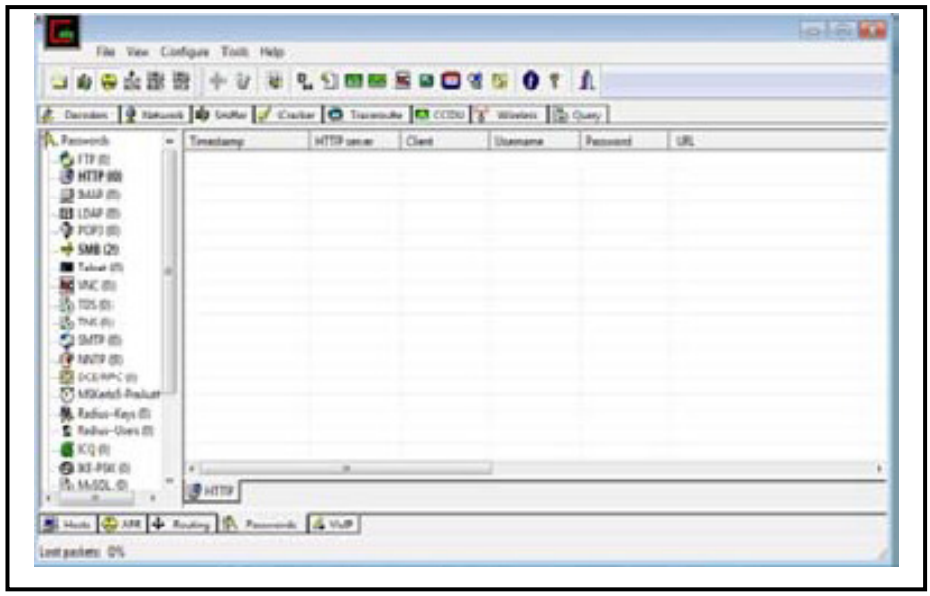
Gambar 23 menunjukkan bahwa ada beberapa penyadapan yang dilakukan pada IP destination 216.185.118.60 dengan menyadap informasi pengambilan *file pixel.gif*.

1.6. Evaluasi Jaringan VPN

Evaluasi jaringan VPN ini dilakukan dengan mengaktifkan kembali *server* VPN dan menjalankan VPN Client dari komputer client.

1.6.1. Pengujian Menggunakan *Software Cain & Abel*

Pada eksperimen ini dilakukan sniffing pada jaringan VPN di PT Layar Sentosa Shipping Corp. dengan menggunakan *software Cain & Abel*.

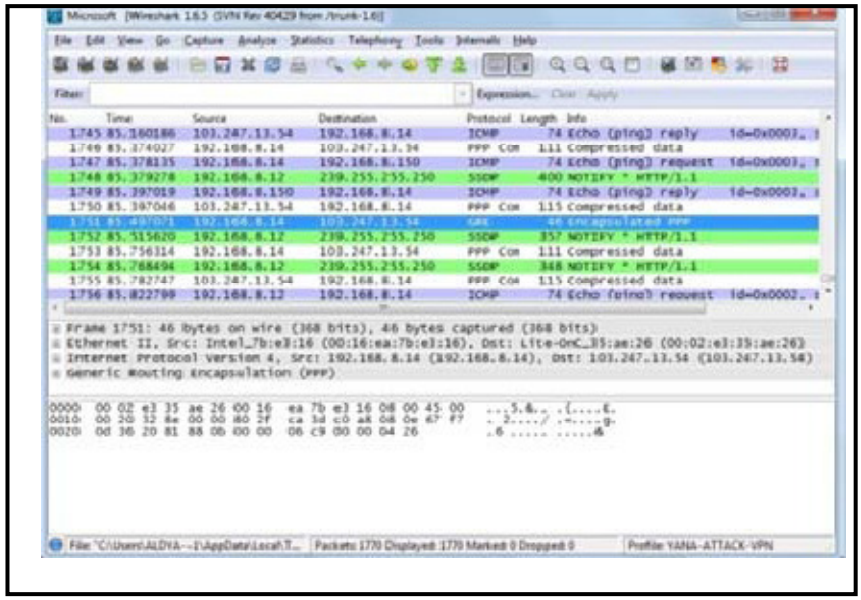


Gambar 4.21 : Cain & Abel pada Jaringan VPN

Gambar 24 menunjukkan bahwa tidak ada aktifitas pada jaringan yang tersedia *hotspot*, karena *client* yang ada sedang berada dalam *tunnel* jaringan VPN.

1.6.2. Pengujian Menggunakan software Wireshark

Pada eksperimen ini dilakukan *sniffing* pada jaringan VPN di PT Layar Sentosa Shipping Corp. dengan menggunakan software Wireshark.



Gambar 4.22 : Wireshark pada Jaringan VPN

Gambar 4.22 menunjukkan bahwa aktivitas *client* dengan IP address 192.168.8.14 telah berjalan di jaringan *tunnel* VPN. Hal ini ditunjukkan pada kolom ino tertera *Encapsulated* PPP dan *Compressed Data*.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Berdasarkan hasil penelitian dari beberapa eksperimen pengujian di atas, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Hasil pengujian konektivitas jaringan VPN:
    a. *Packet Loss*: konektivitas antara kantor Semarang dan kantor pusat Jakarta lebih baik (dengan tingkat *packet loss* 4%) daripada konektivitas antara kantor Semarang dan kantor Surabaya (dengan tingkat *packet loss* 5%).
    b. *Round Trip Time*: *round trip time* dari kantor Semarang ke kantor Jakarta lebih singkat (RTT: 24 *millisecond*) daripada *round trip time* dari kantor Semarang ke kantor Surabaya (RTT: 42 *millisecond*).
    c. FTP *Transfer*: semakin besar *bandwidth* maka proses transfer *file* juga akan semakin cepat. Selain itu, penulis sangat menyayangkan karena selama ini fasilitas FTP *server* tidak diaktifkan. Padahal dari sisi keamanan, fasilitas ini bisa diamankan dengan *login username* dan *password*.
2. Hasil pengujian keamanan jaringan VPN:
    a. *Denial of Service* (DoS) dengan *pingflood attack*: berhasil menyerang dan mengganggu aktivitas jaringan di *server* VPN PT Layar Sentosa Shipping Corp.
    b. *Man-In-the-Middle* (MITM) *Attack*: *attacker* (penyerang) berhasil melakukan *spoofing* terhadap komputer *client* dengan IP *address*: 10.252.108.208 yang sedang bertukar data dengan *server* dengan IP *address*: 10.252.108.127. Hal ini terbukti dari berubahnya MAC Number *client* dari 00:00:e2:9b:3c:b8 menjadi 00:e0:7d:dd:50:0e dan MAC Number *server* dari 00:e0:7d:dd:50:0f menjadi 00:e0:7d:dd:50:0e.
    c. *Hacking* Menggunakan *Linux Bactrack*: *attacker* (penyerang) berhasil membaca *username* dan *password* VPN dari salah satu komputer *client*.
3. Evaluasi Jaringan VPN dan Non-VPN menunjukkan hasil bahwa aktifitas di jaringan VPN lebih baik daripada Non-VPN karena aktivitas yang dilakukan di dalam *tunnel* VPN tidak diketahui oleh orang lain.
4. Kriptografi yang digunakan PT Layar Sentosa Shipping Corp. adalah CISCO *Guard* XT & CISCO *Traffic Anomaly Detector* XT yang merupakan paket layanan yang diberikan oleh PT Indosat Tbk sebagai operator telekomunikasi. CISCO *Guard* XT & CISCO *Traffic Anomaly Detector* XT mampu mendeteksi serangan DoS, DDoS, worm dan jenis serangan lainnya dengan cara memblokir lalu-lintas serangan dan mencegah setiap jenis serangan terhadap jaringan komputer. Ketika CISCO *Traffic Anomaly Detector* XT mengidentifikasi potensi serangan, ia akan menginformasikannya kepada CISCO Guard XT untuk mulai mengalihkan lalu-lintas data yang menjadi target serangan tersebut.

4.2 Saran

Dalam penelitian ini ditemukan beberapa kelemahan, sehingga dalam pengembangan ke depan perlu memperhatikan hal-hal sebagai berikut:

1. Solusi untuk mengatasi permasalahan kelemahan jaringan di PT. Layar Sentosa Shipping adalah dengan meningkatkan pengamanan di level *server* dan *gateway/router*-nya dengan memasang aplikasi *anti flooding*.
2. Perlunya pembenahan pada *security* jaringan dan manajemen *password*-nya. Solusinya sementar adalah dengan cara dibuat dengan kombinasi huruf dan angka serta *password*-nya dibuat lebih dari 10 digit dan terdiri dari kombinasi huruf dan angka. Hal ini bertujuan untuk menyulitkan aksi *generate key* oleh *attacker* (penyerang).
3. Perlunya merubah kebiasaan *user* yang suka menggunakan *username* dan *password* dengan jumlah digit pendek, karena hal ini rentan terhadap penyadapan oleh orang yang tidak berhak (MITM).

DAFTAR PUSTAKA

Chou. 2008, *Strong User Authentication on the Web. United State: Microsoft Corporation.*

Frankel S. et. al. 2005. *Guide to IPSec VPN.National Institute of Standards and Technology*. Departemen Komersial Amerika Serikat.

Madjid. N. 2010, *Perbandingan Ssl (Secure Socket Layer)Dan Ipsec (Internet Protocol Security) Pada Vpn (Virtual Private Network).* Surabaya: *Electrical Engineering Polytechnic Institute of Surabaya* (EEPIS).

Sari M.W. 2011, Analisis Keamanan Jaringan Virtual Private Network (VPN) pada Sistem Online Microbanking (Kasus di BMT Al Ikhlas Yogyakarta). Universitas Gadjah Mada. Yogyakarta.

Sukaridhoto.S. 2005. *Teknik Keamanan Pada Voip Dengan Virtual Private Networking Dan Kriptografi Serta Korelasi Terhadap Bandwidth Dan Intelligibility Suara,* Surabaya: *Electrical Engineering Polytechnic Institute of Surabaya* (EEPIS).

Thomas, Tom. 2005. *Network Security First Step.* Penerbit Andi, Yogyakarta.