EVALUASI IMPLEMENTASI KEAMANAN JARINGAN VIRTUAL PRIVATE NETWORK (VPN) (STUDI KASUS PADA CV. PANGESTU JAYA)

Yana Hendriana
Jurusan Teknik Informatika
Fakultas Teknologi Industri Universitas Ahmad Dahlan Yogyakarta
yanahendri@uad.ac.id, yanahendri@gmail.com

ABSTRACT

CV. Pangestu Jaya are engaged in the procurement of goods and services as well as software house, in the delivery of important company data, between the head office and branches in other cities online using VPN. The research was carried out with due diligence scenarios based on user needs. Tests are performed Connectivity Testing, Testing Data Transfer, VPN Attacking with DoS (Denial Of Services), Hacking VPN with ARP Poisoning in Linux Backtrack. The results of experimental testing of attacking with Denial of Service (DoS) using pingflood tool was successfully shut down service / services on the VPN server. Besides testing hacking / ARP Poisoning to obtain a username and password by using the tools of the Linux backtrack also broke through the client login access to the server.

Keywords : vpn, attacking, poisoning, hacking, connectivity.

INTISARI

CV. Pangestu Jaya yang bergerak di bidang pengadaan barang dan jasa serta software house, dalam pengiriman data penting perusahaan, antara kantor pusat dengan kantor cabang di kota lain secara online menggunakan jaringan VPN. Penelitian ini dilakukan dengan skenario uji kelayakan berdasarkan kebutuhan *user*. Pengujian-pengujian yang dilakukan adalah Pengujian Konektivitas, Pengujian *Transfer Data, Attacking* VPN dengan DoS (*Denial Of Services*), *Hacking VPN* dengan *ARP Poisoning* di *Linux Backtrack.* Hasil eksperimen pengujian *attacking* dengan *Denial of Service (DoS)* menggunakan *tool pingflood* ternyata berhasil mematikan service/layanan pada VPN *server.* Selain itu pengujian *hacking / ARP Poisoning* untuk mendapatkan *username* dan *password* dengan menggunakan *tools* yang ada pada Linux *backtrack* juga berhasil menembus akses login *client* ke *server*.

Kata kunci : vpn, attacking, poisoning, hacking, konektivitas.

A. PENDAHULUAN

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

CV. Pangestu Jaya yang bergerak di bidang pengadaan barang dan jasa serta *software house*, dalam pengiriman data berupa data keuangan, data kepegawaian, data *update program* terbaru*,* antara kantor pusat dengan kantor cabang di kota lain secara *online* membutuhkan sistem yang memiliki tingkat keamanan pengiriman data yang tinggi, yaitu jaringan VPN, karena data yang dikirim bersifat rahasia dan pihak selain yang memiliki hak akses tidak boleh mengaksesnya. Sebelum menggunakan VPN, CV. Pangestu Jaya masih menggunakan email untuk pengiriman data-data perusahaan hingga pada suatu ketika terjadi masalah yaitu email yang dikirim berhasil diacak-acak/diganggu oleh orang yang tidak berkepentingan karena orang tersebut mengetahui *password* dari alamat email penerima sehingga hal tersebut mengakibatkan bocornya data-data penting perusahaan yang dikirim via email, oleh karena itu CV. Pangestu Jaya melakukan implementasi jaringan VPN untuk meningkatkan keamanan data-data penting perusahaan. Untuk itu, jaringan vpn ini masih diperlukan uji coba kestabilan konektivitas jaringan VPN yang diimplementasikan. Implementasi jaringan VPN ini dipastikan

akan mengalami banyak gangguan, maka perlu dilakukan evaluasi melalui beberapa pengujian keamanan untuk mengetahui faktor-faktor yang mempengaruhi implementasi keamanan jaringan VPN yang ada di CV. Pangestu Jaya.

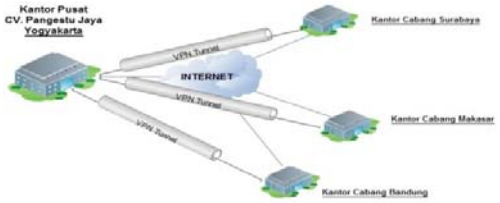
Kontribusi dari penelitian ini adalah untuk membantu CV. Pangestu Jaya dalam mengevaluasi kinerja jaringan VPN dalam melindungi data-data sensitif yang dikirim maupun diterima antar kantor cabang melalui *internet* serta memberikan rekomendasi untuk perbaikan atau tindakan lebih lanjut

Batasan pada penelitian ini adalah sebagai berikut.

a. Penelitian ini hanya membatasi pada evaluasi fungsi dan manfaat jaringan *Virtual Private Network* (VPN) bukan pada perancangan atau pembuatan *software* pendukung vpn.

b. Penelitian ini hanya pada pengujian keamanan dalam komunikasi data untuk mengetahui faktor-faktor yang mempengaruhi keamanan komunikasi data pada jaringan VPN di CV. Pangestu Jaya bukan pada VoIP maupun *streaming.*

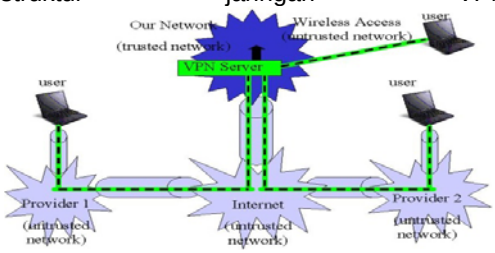
Jaringan vpn ini dimanfaatkan untuk menghubungkan antara kantor pusat dengan beberapa kantor cabang, dengan diagram topologi jaringan vpn yang digunakan oleh CV. Pangestu Jaya pada Gambar 1.



Gambar 1. Diagram Topologi Jaringan VPN

B. LANDASAN TEORI

Virtual Private Network (VPN) adalah teknik pengaman jaringan yang bekerja dengan cara membuat suatu *tunnel* sehingga jaringan yang terpercaya dapat terhubung dengan jaringan yang ada di luar melalui *internet*. Gambar 2 menggambarkan tentang struktur jaringan VPN.



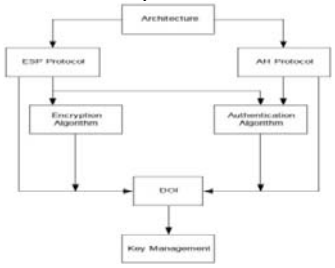
Gambar 2. Struktur Jaringan VPN (Sukaridhoto, 2005)

1. Kriptografi pada VPN

VPN menggunakan dua bentuk kriptografi, yaitu kriptografi kunci simetris dan kriptografi kunci publik. Kriptografi kunci simetris biasanya lebih efisien dan membutuhkan biaya pemrosesan yang lebih murah bila dibandingkan dengan kriptografi kunci publik. Oleh karena itu, kriptografi kunci simetri lebih sering digunakan untuk mengenkripsi bagian terpenting dari data yang akan dikirimkan melalui VPN. Algoritma yang umumnya digunakan untuk implementasi kriptografi kunci simetris meliputi *Digital Encryption Standard* (DES), *Triple DES* (3DES), *Advanced Encryption Standard* (AES), *Blowfish, RC4, International Data Encryption Algorithm* (IDEA), dan *Hash Message Authentication Code* (HMAC) versi *Message Digest* 5 (MD5) dan *Secure Hash Algorithm* (SHA-1). Algoritma yang umumnya digunakan untuk algoritma kunci publik adalah meliputi RSA, *Digital Signature Algorithm* (DSA), dan *Elliptic Curve DSA* (EDBSA) (Frankel, 2005).

2. Arsitektur Protokol IPSec

IPSec protokol yang dikombinasikan dengan algoritma *default*-nya didesain untuk menyediakan keamanan lalu lintas internet yang baik. Bagaimanapun juga keamanan yang diberikan oleh protokol ini sebenarnya bergantung pada kualitas dari implementasi. Perkembangan arsitektur IPsec mengacu pada pokok persoalan yang terdapat pada RFC. Terdapat tujuh bagian utama pada Gambar 3 yang dapat digunakan untuk mendefinisikan keseluruhan arsitektur dari Ipsec (Thomas, 2005).



Gambar 3. Arsitektur IP *Secure*

3. Teknologi *Tunneling*

Teknologi *tunneling* adalah teknologi yang bertugas untuk menangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Disebut *tunnel* karena koneksi *point-to-point* tersebut sebenarnya terbentuk dengan melintasi jaringan publik (*internet)*, tetapi koneksi tersebut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan publik tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya. Teknologi vpn ini sama dengan penggunaan jalur *busway* yang pada dasarnya menggunakan jalan raya sebagai jalur umum/publik, tetapi dia membuat jalur sendiri untuk dapat dilalui bus khusus.

4. 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 pintu yang tidak dikunci sehingga dapat masuk dengan mudah.

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.

c. Packet Sniffer

Packet sniffer adalah sebuah program yang menangkap (*capture*) data dari paket yang lewat di jaringan. Data tersebut bisa 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.*

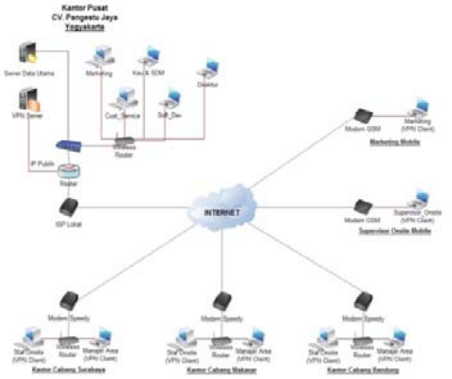
d. Denial of Service (DoS)

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'.*

5. Jenis implementasi VPN

Dilihat dari jenis implementasi VPN yang ada, dalam penelitian ini termasuk dalam kategori *Site-to-site* VPN. *Site-to-site* VPN merupakan jenis implementasi VPN yang menghubungkan antara dua tempat atau lebih yang letaknya berjauhan, seperti halnya menghubungkan kantor pusat dengan kantor cabang, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan kantor pusat dengan kantor cabang suatu perusahaan disebut *intranet site-to-site* VPN.

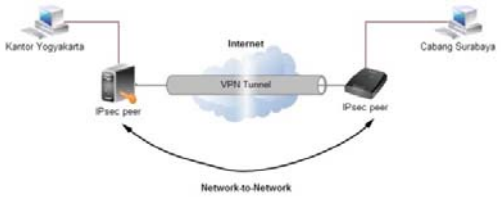
Topologi jaringan *site-to-site* VPN ditunjukkan pada Gambar 4.



Gambar 4. Topologi jaringan *site-to-site* VPN

6. Protokol yang digunakan dalam VPN

Dalam penelitian ini 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, Gambar 5. menunjukkan cara kerja IP Security pada *site-to-site* VPN.



Gambar 5. Cara kerja IP Sec *Network-to-Network*

C. METODE PENELITIAN

Penelitian ini dilakukan dengan metode yang terdiri dari beberapa tahap. Tahap-tahap tersebut adalah sebagai berikut:

1. Studi Literatur
   Tahap ini dilakukan untuk mencari dan mempelajari sumber-sumber informasi dari beberapa artikel dan jurnal yang berkaitan dengan keamanan jaringan vpn. Tahap ini sangat penting untuk membangun pengertian yang benar dan memadai untuk melakukan penelitian.
2. Wawancara
   Tahap selanjutnya adalah wawancara terhadap narasumber yang memiliki data-data operasional perusahaan pada jaringan komputer dan internet. Wawancara ini dilakukan untuk mendapatkan informasi yang mendasari penelitian ini.
3. Eksperimen pengujian
   Tahap ini dilakukan untuk melakukan beberapa pengujian jaringan vpn, yaitu pada stabilitas koneksi jaringan vpn dan untuk pengujian pada keamanan jaringan vpn.

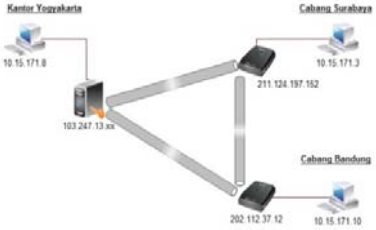
Langkah-langkah penelitian

1. Observasi
2. Identifikasi & rumusan masalah
3. Persiapan Hardware, Instalasi OS, konfigurasi LAN
4. Instalasi Aplikasi attacking & hacking
5. Pengujian konektivitas
6. Pengujian attacking & hacking
7. Analisis & Identifikasi kelemahan
8. Dokumentasi Hasil Penelitian
9. Membuat laporan Penelitian

D. HASIL DAN PEMBAHASAN

1. Eksperimen *Network Setup* dan Tes Kondisi

Tes Kondisi dilakukan dengan cara *traceroute* langsung ke IP *Virtual* Bandung, hasilnya adalah 10.15.171.3 (IP *Virtual* Surabaya) dan 10.15.171.10 (IP *Virtual* Bandung). Area jaringan yang dilakukan pengujian adalah VPN Kantor Pusat Yogyakarta, cabang Surabaya dan cabang Bandung, Gambar 6. menunjukkan area pengujian jaringan vpn.



Gambar 6. Area pengujian jaringan VPN

2. Uji Konektivitas Jaringan

Uji konektivitas yang dilakukan melalui kantor pusat Yogyakarta, dengan kantor cabang Bandung dan kantor cabang Surabaya pada tanggal 31 Maret 2012 pada pukul 13.00 sampai dengan pukul 16.00 menggunakan konfigurasi alamat IP sebagai berikut.

a. IP PUBLIK CV. Pangestu Jaya Pusat Yogyakarta:
   IP : 103.247.1x.xxx
   Subnet Mask : 255.255.255.252
   Default Gateway : 103.247.1x.xxx
b. IP *Speedy* kantor cabang Surabaya:
   IP : 211.124.197.152
   Subnet Mask : 255.255.255.240
   Default Gateway : 211.124.197.117
c. IP *Speedy* kantor cabang Bandung:
   IP : 202.112.37.12
   Subnet Mask : 255.255.255.224
   Default Gateway : 202.112.37.30

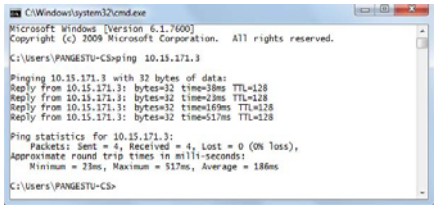
Eksperimen uji konektivitas diawali dengan terlebih dahulu menjalankan *software vpn client*. Setelah itu muncul tampilan masukan nama komputer server VPN dan IP publiknya lalu *connect* untuk masuk atau tombol *exit* untuk keluar, tampilannya dapat dilihat pada Gambar 7.

Gambar 7. *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 8.

Gambar 8. Tampilan *Login User*

Uji konektivitas dengan cara dilakukan *ping* dari komputer kantor pusat Yogyakarta ke komputer cabang Surabaya ditunjukkan pada Gambar 9.



Gambar 9. Hasil *ping* ke komputer Surabaya

3. Mekanisme Pengujian Konektivitas

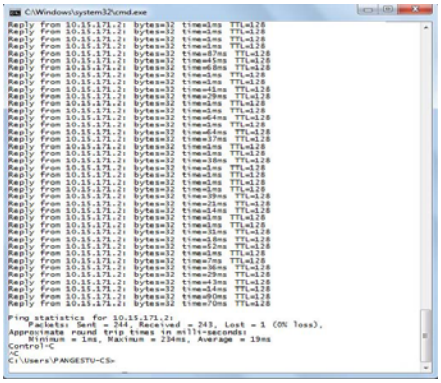
Mekanisme Pengujian konektivitas pada penelitian ini dilakukan dengan beberapa parameter yaitu:

1. *packet loss;*
2. *round trip;*
3. *ftp transfer.*

Berikut ini penjelasan paramater pengujian konektivitas.

1. *Packet Loss*

Eksperimen pengujian ini untuk memantau rata-rata, minimum dan maksimum *packet loss* yang melalui *tunnel* VPN. Di setiap lokasi pengujian berikut dilakukan 30 kali tes dengan masing-masing tes selama 5 menit menggunakan *stopwatch* dan rata-rata diatas 200 *packet*. Salah satu contoh tampilan hasil ping ditunjukkan pada Gambar 10.



Gambar 10. Eksperimen *Packet Loss* dan *Round Trip*

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

Tabel 1. *Packet loss* pada *tunnel* VPN

Lokasi Pengujian	IP sumber	IP tujuan	Min. Packet Loss	Max. Packet Loss	Rata-rata Packet Loss
Kantor Pusat	10.15.171.13	10.15.171.2	0	1	0,37
Kantor Bandung	10.15.171.17	10.15.171.2	1	7	2,67
Modem Fleksi	10.15.171.25	10.15.171.2	5	13	8,20

Tabel 1. menunjukkan bahwa konektivitas jaringan VPN di kantor pusat jauh lebih baik dibanding dengan koneksi kantor cabang dan mengunakan modem fleksi. Komputer yang digunakan untuk melakukan *PING* ke *server* data dengan ip tujuan 10.15.171.2. dari 30 kali tes *ping* diperoleh *Min. Packet Loss* 0 dan *Max. Packet Loss* 1 dengan rata-rata *packet loss* 0,37. Hal ini menunjukkan adanya *loss* dengan jumlah sedikit, kemungkinan karena masih dalam jaringan dan *router* yang sama. Hasil tes dari kantor cabang Bandung yang menggunakan jaringan *Telkom Speedy* dari 30 kali tes diperoleh *Min. Packet Loss* 1 dan *Max. Packet Loss* 7 dengan rata-rata *packet loss* 2,67. Hasil tes menggunakan *modem Telkom fleksi* dari 30 kali tes diperoleh diperoleh *Min. Packet Loss* 5 dan *Max. Packet Loss* 13 dengan rata-rata *packet loss* 8,20.

2.*Round trip*

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.

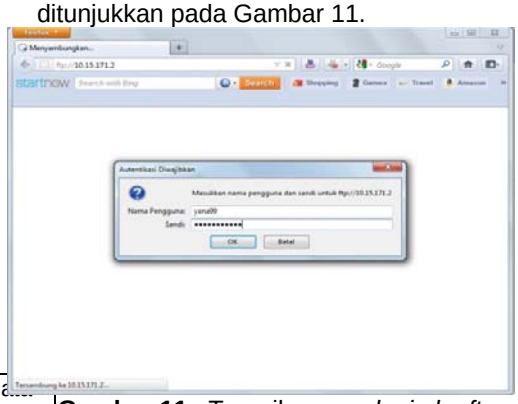
Tabel 2. *Round trip* pada *tunnel* VPN

Lokasi Pengujian	IP sumber	IP tujuan	Min. waktu dalam milisecond	Max. waktu dalam milisecond	Rata-rata waktu dalam milisecond
Kantor Pusat	10.15.171.9	10.15.171.2	10 ms	31 ms	20 ms
Kantor Bandung	10.15.171.21	10.15.171.2	56 ms	131 ms	96 ms
Modem Fleksi	10.15.171.14	10.15.171.2	124 ms	242 ms	180 ms

Tabel 2. menunjukkan hasil dari *round trip* yang telah dilakukan pada proses *ping* dari 30 kali tes diambil hasil *round trip* yang paling kecil dan round trip yang paling besar dalam hitungan *millisecond.* Dari 30 kali tes *ping* untuk lokasi pengujian di kantor pusat diperoleh *Min. round trip* 10ms dan *Max. round trip* 31ms dengan rata-rata *round trip* 20ms. Kemudian untuk hasil tes dari kantor cabang Bandung yang menggunakan jaringan *Telkom Speedy* dari 30 kali tes diperoleh *Min. round trip* 56ms dan *Max. round trip* 131*ms* dengan rata-rata *round trip* 96*ms.* Sedangkan untuk hasil tes menggunakan *modem Telkom fleksi* dari 30 kali tes diperoleh diperoleh *Min. round trip* 124ms dan *Max. round trip* 242*ms* dengan rata-rata *round trip* 180ms*.*

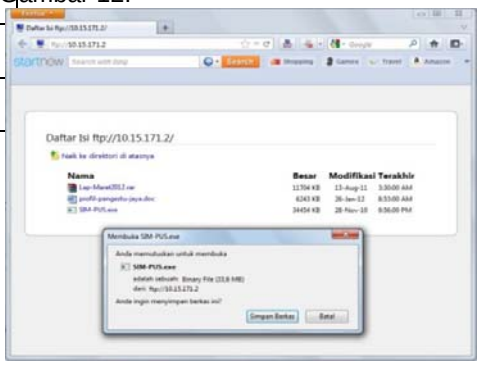
3. FTP *Transfer*

Eksperimen pengujian ini diharapkan bisa mengetahui waktu yang dibutuhkan untuk *transfer 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 via ftp dalam jaringan VPN maka dalam penelitian ini dicoba untuk mengaktifkan FTP *server* untuk sementara waktu dengan pengaturan *username* dan *password* demi keamanan, hal itu ditunjukkan pada Gambar 11.



Gambar 11. Tampilan *user login ke ftp server*

Eksperimen ini file yang dicoba untuk *download* adalah file SIM-PUS.exe yang berukuran 33,6 MB yang ditunjukkan pada Gambar 12.



Gambar 12 *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 3.

Tabel 3. File *Transfer* via FTP pada *tunnel* VPN

Lokasi Pengujian	IP sumber	IP tujuan	Waktu Transmisi
Kantor Pusat	10.15.171.9	10.15.171.2	00:00:09:21
Kantor Bandung	10.15.171.21	10.15.171.2	00:26:51:33
Modem Fleksi	10.15.171.14	10.15.171.2	00:55:11:29

Tabel 3. menunjukkan bahwa waktu yang diperlukan untuk *transfer/download* file di kantor pusat = 00:00:09:21 yaitu 9 detik 21 milidetik, untuk kantor Bandung waktu yang dipakai untuk *download* = 00:26:51:33 yaitu 26 menit 51 detik 33 milidetik, sedangkan dengan menggunakan modem fleksi = 00:55:11:29 yaitu 55 menit 11 detik 29 milidetik. Dari eksperimen *download via ftp* tersebut dapat disimpulkan bahwa kecepatan *transfer* filenya dipengaruhi oleh *bandwidth* yang tersedia di masing-masing komputer *client.*

Kesimpulan dari beberapa eksperimen *packet loss* tersebut menunjukkan jaringan yang paling stabil adalah konektivitas jaringan yang ada di kantor pusat, urutan kedua menggunakan *Telkom speedy* di kantor Bandung dan urutan terakhir menggunakan modem fleksi. Hal ini menunjukkan bahwa tingkat konektivitas jaringan dipengaruhi oleh ketersediaan *bandwidth* yang tersedia di komputer *client.*

4. Mekanisme Pengujian Keamanan

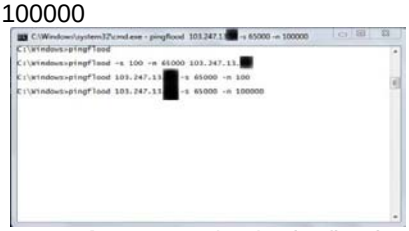
Mekanisme pengujian keamanan pada penelitian ini dilakukan dengan beberapa parameter, yaitu:

a. Attack* menggunakan *Denial of Service (DoS)

Pengujian untuk melakukan *attack* pada komputer *server* menggunakan metode *Denial of Service.* Eksperimen *Denial of Service* bertujuan untuk menghentikan atau mematikan *service* pada komputer target dalam hal ini *server* VPN. *Denial of Service (DoS)* dengan aplikasi *pingflood.exe*

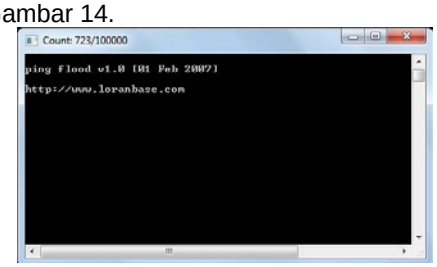
IP address target yang akan diserang adalah ip publik server vpn (103.247.1x.xxx).

- Command Prompt diaktifkan dengan start > run > cmd
- Langkah selanjutnya dilakukan perintah:
  pingflood 103.247.1x.xx –s 65000 –n 100000



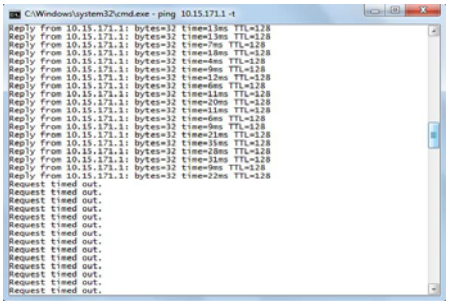
Gambar 13. Perintah *pingflood*

Gambar 13 menunjukkan perintah *pingflood* yang diarahkan pada ip target, selanjutnya muncul tampilan indikator proses *pingflood* yang ditunjukkan pada Gambar 14.



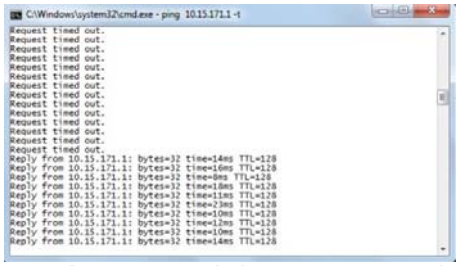
Gambar 14. Indikator proses *counter pingflood*

Gambar 14. menunjukkan proses *counter* yang telah mencapai 723 paket dari total 100000 paket yang dikirimkan melalui perintah *pingflood.* Efek dari *attack* dengan *pingflood* ini 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 15.



Gambar 15 Efek *pingflood attack*

Proses *pingflood attack* akan berhenti setelah jumlah paket *pingflood* yang dikirimkan telah terpenuhi yaitu 100000 paket maka koneksi ke ip target normal kembali, yang ditunjukkan pada Gambar 16.



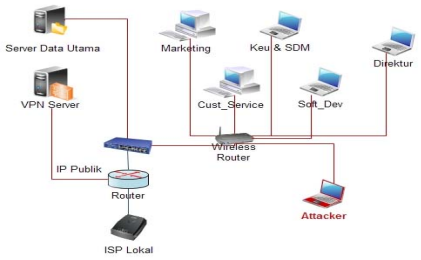
Gambar 16. Koneksi IP Target Normal

Denial of Service (DoS) Attack 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 CV. Pangestu Jaya, hal ini merupakan salah satu kelemahan jaringan di CV. Pangestu Jaya. Solusi untuk mengatasi permasalahan kelemahan jaringan di CV. Pangestu Jaya adalah dengan meningkatkan pengamanan di level *server* dan *gateway/router*-nya.

b. *Man-in-the-middle-attack* atau MIMA

Man-in-the-middle-attack atau MIMA adalah salah satu serangan pada jaringan dengan akses terbuka misalnya *HOTSPOT*. Dengan cara ini akan dilakukan penyadapan *username* dan *password* dengan menggunakan ***Linux Backtrack***. Cara *Man-in-the-middle-attack* dapat dilakukan jika komputer *attacker* berada di dalam satu *network* dengan beberapa komputer yang lainnya sesuai dengan namanya *Man-in-the-middle-attack*. Hal ini ditunjukkan pada Gambar 17.



Gambar 17. MIMA (*Man In The Middle Attack)*

c. *Hack* menggunakan *Linux Backtrack*

Eksperimen *Hack* menggunakan *Linux Backtrack* tujuannya untuk mendapatkan *username* dan *password* yang digunakan oleh *user/client* pada saat koneksi ke *server* vpn.

Setting ip *address* jaringan vpn yang akan di-*hack, sebagai berikut*.

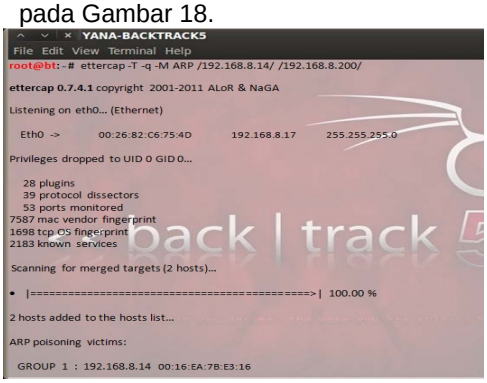
– ip *server* vpn 103.247.1x.xx
– *gateway* LAN 192.168.8.200
– ip *attacker* 192.168.8.17
– ip *client target* 192.168.8.14

Teknik ini biasa dinamakan dengan arp poisoning. Tools yang digunakan adalah ettercap yang secara bawaan sudah tersedia di Linux Backtrack, *attacker* menggunakan ettercap pada mode text.

contoh sintaxnya adalah: ettercap -T -q -M ARP /ip target/ /ip gateway/ atau ettercap -T -q -M ARP /192.168.8.14/ /192.168.8.200/

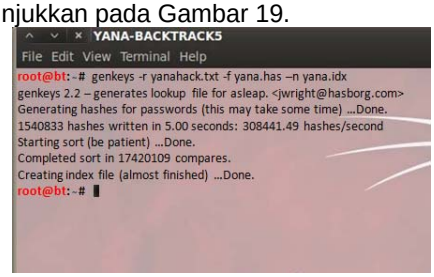
– *option* -T : mode text
– *option* -q : ettercap dijalankan pada keadaan tenang/outputnya tidak terlalu banyak
– *option* -M : menggunakan teknik ARP poisoning

Penerapan dari sintax tersebut ditunjukkan pada Gambar 18.



Gambar 18. *Sintax ettercap*

Hacking pada Linux *Backtrack* ini ini menggunakan teknik *bruteforce* dengan menggunakan file kamus (*wordlist.txt*/ 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 19.



Gambar 19. *Sintax genkeys*

Gambar 19. menunjukkan hasil berupa file yana.has dan yana.idx
– options -r : meminta inputan dari sebuah file (dalam hal ini file wordlist)
– options -f : akan membuat output dari file wordlist menjadi file2 hash
– options -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 program *asleap*. tapi yang digunakan adalah *asleap* bawaan dari backtrack 5. Hal ini ditunjukkan pada Gambar 20.

Gambar 20. *Sintax asleap*

Gambar 20. menunjukkan adanya beberapa *option* yang digunakan, yaitu:

– options -i : menunjukkan interface/ ethernet yang di gunakan, misalnya eth0

– options -f : meminta inputan dari file hash yang sudah dibuat

– options -n : meminta inputan dari fle index yang sudah dibuat

Ketika target melakukan koneksi ke server vpn, maka bisa dilihat *output capture* koneksinya sehingga dapat dilihat username dan password yang dilakukan oleh user di komputer target, hasil *capture*-nya ditunjukkan pada Gambar 21.

Gambar 21. *Capture username dan password*

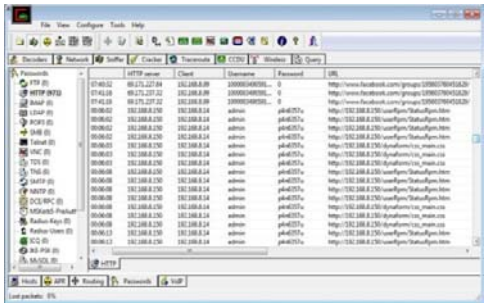
Berdasarkan eksperimen pengujian *hack* dengan menggunakan Linux *backtrack,* maka dapat disimpulkan bahwa keamanan jaringan vpn di CV. Pangestu Jaya masih ada kelemahan karena masih bisa di-*hack pada username* dan *password-nya* dengan menggunakan *Linux Backtrack.* Oleh karena itu, jaringan VPN yang telah diimplementasikan masih perlu pembenahan pada *security* jaringan dan manajemen *password*-nya*.*

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. Pengujian menggunakan *software Cain & Abel*

Eksperimen ini mencoba dilakukan *sniffing* pada jaringan non VPN di CV. Pangestu Jaya dengan menggunakan *software cain & Abel.*

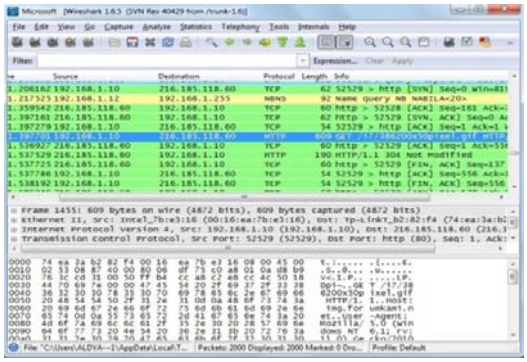


Gambar 22. Cain & Abel pada jaringan Non VPN

Gambar 22 menunjukkan bahwa ada beberapa penyadapan yang dilakukan pada ip acces point dengan terlihat username dan password.

2. Pengujian menggunakan *software Wireshark*

Eksperimen ini mencoba dilakukan *sniffing* pada jaringan non VPN di CV. Pangestu Jaya dengan menggunakan *software Wireshark.*



Gambar 23. *Wireshark* pada jaringan Non VPN

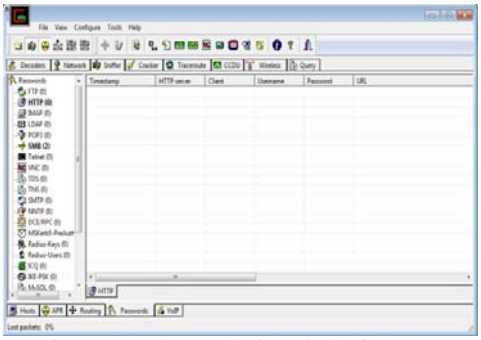
Gambar 23. menunjukkan bahwa ada beberapa penyadapan yang dilakukan pada ip destination 216.185.118.60 dengan menyadap informasi pengambilan file pixel.gif.

6. Evaluasi Jaringan VPN

Evaluasi Jaringan VPN ini dilakukan dengan mengaktifkan kembali *server* VPN dan menjalankan *vpn client* dari komputer *client.*

1. Pengujian menggunakan *software Cain & Abel*

Eksperimen ini mencoba dilakukan *sniffing* pada jaringan VPN di CV. Pangestu Jaya dengan menggunakan *software cain & Abel.*

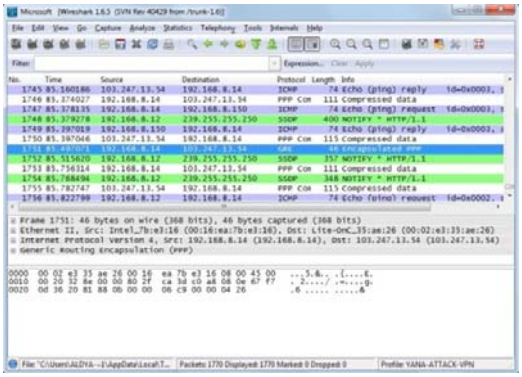


Gambar 24 Cain & Abel pada jaringan VPN

Gambar 24 menunjukkan bahwa tidak ada aktivitas pada jaringan yang tersedia di HOTSPOT, karena *client* yang ada sedang dalam tunnel jaringan VPN.

2. Pengujian menggunakan *software Wireshark*

Eksperimen ini mencoba dilakukan *sniffing* pada jaringan VPN di CV. Pangestu Jaya dengan menggunakan *software Wireshark.*



Gambar 25 *Wireshark* pada jaringan VPN

Gambar 25 menunjukkan bahwa aktivitas client vpn dengan ip *address* 192.168.8.14 telah berjalan di jaringan *tunnel* vpn, hal itu ditunjukkan pada kolom info yang tertera *Encapsulated* PPP dan *Compressed* data.

E. KESIMPULAN DAN SARAN

1. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan beberapa eksperimen pengujian, maka dihasilkan beberapa kesimpulan sebagai berikut.

a. Hasil pengujian konektivitas jaringan vpn antara kantor pusat dengan kantor cabang di CV. Pangestu Jaya bisa berjalan dengan baik dan stabil, dengan tingkat loss dan round trip dalam jumlah kecil, tetapi tetap dipengaruhi oleh *bandwidth* yang dimiliki oleh masing-masing komputer *client.* Eksperimen *transfer* file via FTP sudah cukup baik, tetapi masih disayangkan karena selama ini fasilitas FTP *server* tidak diaktifkan, padahal dari sisi keamanan fasilitas ini bisa diamankan dengan *login user* dan *password*.

b. Hasil Pengujian keamanan menunjukkan masih adanya kelemahan terhadap serangan *Denial of Service (DoS) dengan pingflood attack.* Selain itu *j*aringan VPN masih rentan terhadap serangan penyusup, dengan telah dibobolnya *username* dan *password* vpn melalui eksperimen *hacking* menggunakan Linux *Backtrack*.

c. Evaluasi Jaringan VPN dan Non VPN menunjukkan hasil bahwa aktivitas di jaringan VPN lebih baik dari pada Non VPN karena aktivitas yang dilakukan didalam tunnel VPN tidak diketahui oleh orang lain.

2. SARAN

Dalam penelitian ini ditemukan beberapa kelemahan, sehingga dalam pengembangan kedepan perlu memperhatikan saran sebagai berikut:

a. Solusi untuk mengatasi permasalahan kelemahan jaringan di CV. Pangestu Jaya adalah dengan meningkatkan pengamanan di level *server* dan *gateway/router*-nya dengan memasang aplikasi *anti flooding*.

b. Perlunya pembenahan pada *security* jaringan dan manajemen *password*-nya*.* Solusinya 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 tujuannya untuk menyulitkan aksi generate key oleh *attacker.*

c. Perlunya merubah karakter/kebiasaan *user* yang suka menggunakan *username* dan *password* dengan jumlah digit pendek, karena hal ini rentan terhadap penyadapan oleh orang yang tidak berhak.

DAFTAR PUSTAKA

Braun T., M. Günter, I. Khalil, L. Liu. 2000, *Performance Evaluation of Virtual Private Network*. Universität Bern.

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

Elektro Indonesia. 2001, *Jaringan Privat Virtual Dinamis: Sebuah Jawaban Keamanan untuk Intranet Bisnis*, diambil pada alamat website:

http://www.elektroindonesia.com/elektro/komp35.htm, diakses tanggal 20 Januari 2012.

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).

Meeta G. 2003, *Building a Virtual Private Network*. Premier Press.

Purbo Onno W.. 2001, Keamanan Jaringan Internet. PT. Elex Media Komputindo. Jakarta.

Raharjo.B. 2002. *Keamanan system informasi Berbasis Internet*. Bandung: PT Insan Indonesia.

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.

Schneier B. 1996, *Applied Cryptography : Protocols, Algorithms, and Source Code in C, USA, John Wiley & Sons, Inc*.

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.