ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN PADA PT. DAE MYUNG HIGHNESS INDONESIA

Fariz Alwafi
Program Studi Teknik Informatika STMIK Nusa Mandiri, Bekasi
Jl. Kaliabang No. 8 Perwira Bekasi
Email : alfariz24@gmail.com

ABSTRACT

VPN security with an attack (attacking) the method of Denial of Service (DOS) m Man-in-the-Middle (MITM) with ettercap and hacking with Backtrack Linux applications. The experimental results of testing connectivity to the conclusion that the bandwidth is a major factor merits network connectivity between offices. In experiments testing the VPN security, attack (hacking) to Denial of Service (DoS) was successfully shut down service or service on the VPN server. Security of data in a computer network is very important, especially confidential data. Currently there are several alternative methods for data security on the network, for example to encrypt the data before it is sent, install a firewall so that no external intruders who can get into the internal computer network and others. To overcome the problem of security in data communications on public networks. In general, the VPN is a local communication network connected via the public network, public infrastructure is the most widely used Internet network. Inside there is a combination of technology VPN tunneling and encryption to create a VPN into a reliable technology to solve security problems on the network. VPN itself is highly dependent on the stability of the Internet both in the server and the user, it is necessary to be equipped with the best ISP that provides Internet access speed and security are qualified to anticipate the attack to the VPN server.

Keyword: VPN, connectivity, security, attacking.

ABSTRAK

Keamanan VPN dengan melakukan serangan (*attacking*) dengan metode Denial of Service (DOS) Man-in-the-Middle (MITM) dengan ettercap dan hacking dengan aplikasi Linux Backtrack. Hasil eksperimen pengujian konektivitas memberikan kesimpulan bahwa bandwidth merupakan faktor utama baik-buruknya konektivitas jaringan antar kantor. Pada eksperimen pengujian keamanan VPN, serangan (*attacking*) dengan *Denial of Service* (DoS) ternyata berkasil mematikan service atau layanan pada server VPN. Keamanan data pada sebuah jaringan komputer sangatlah penting, terutama data yang bersifat rahasia. Saat ini terdapat beberapa alternatif metode untuk keamanan data pada jaringan, misalnya dengan engenkripsi data sebelum dikirimkan, memasang firewall sehingga tidak ada penyusup dari luar yang dapat masuk ke jaringan komputer internal dan lain-lain. Untuk mengatasi masalah keamanan dalam komunikasi data pada jaringan umum. Secara umum VPN merupakan suatu jaringan komunikasi lokal yang terhubung melalui media jaringan publik, infrastruktur publik yang paling banyak digunakan adalah jaringan internet. Didalam VPN terdapat perpaduan teknologi tunneling dan enkripsi yang membuat VPN menjadi teknologi yang handal untuk mengatasi permasalahan keamanan didalam jaringan. VPN sendiri sangat tergantung pada kestabilan jaringan internet baik dari sisi Server maupun User, untuk itu perlu dibekali dengan ISP yang terbaik yang menyediakan kecepatan akses internet dan keamanan yang mumpuni guna mengantisipasi serangan kepada VPN Server.

Kata Kunci : VPN, konektivitas, keamanan, *attacking*.

1. Pendahuluan

Kemajuan di bidang teknologi informasi khususnya internet benar-benar berdampak pada aktifitas didalam 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.

Perkembangan di bidang informasi begitu cepat, hal ini diikuti dengan perkembangan teknologi komunikasi khususnya internet. Kehadiran internet di Indonesia sudah sangat di butuhkan mengingat bahwa teknologi informasi ini telah memberikan kemudahan proses komunikasi yakni dengan meniadakan jarak dan waktu yang selama ini di rasakan sebagai faktor penghambat. Maka dari itu, diperlukan sebuah jaringan yang dapat digunakan sebagai sarana untuk mengakses internet maupun saling bertukar informasi.

PT Dae Myung Highness Indonesia adalah perusahaan yang bergerak di bidang elektronik yang memiliki cabang di kota lain. Oleh karena itu menjadi suatu keharusan untuk dapat membangun sebuah jaringan yang dapat mengintegrasikan seluruh kantor cabang yang ada secara *realtime*. Selama ini perusahaan masih manual dalam bertukar data dan akses ERP Sistem dilakukan di kantor pusat. Permasalahan yang muncul adalah faktor keamanan jaringan yang menjadi perhatian khusus.

Teknologi *private network* adalah suatu komunikasi dalam jaringan sendiri yang terpisah dari jaringan umum. Penelitian ini menganalisis dan mengimplementasikan keamanan jaringan dengan merancang VPN berbasis PPTP dengan Mikrotik Router Operating System.

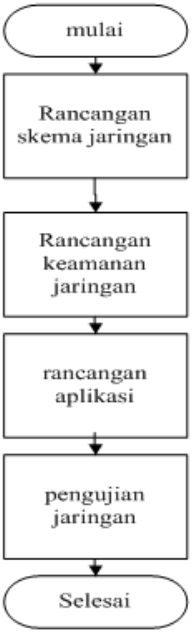
2. Bahan Dan Metode Penelitian

2.1. Bahan

Pada penelitian ini digunakan beberapa perangkat lunak dan perangkat keras. Perangkat lunak yang digunakan meliputi Microsoft Windows 2000 Server. Adapun perangkat keras pada *server* yaitu processor Intel Pentium dual core 3.0 GHz, memory DDRIII 4 GB, 1 buah harddisk Seagate 500Gb 7200 rpm dan NIC 3Com Fast Etherlink 10/100 Mbps. Sedangkan perangkat keras pada user yaitu processor Intel Pentium Dual Core 3.0 GHz, memory DDRIII 2 GB, harddisk Seagate 320Gb dan NIC 3Com Fast Etherlink 10/100 Mbps serta switch dan kabel.

2.2. Metode Penelitian

Penelitian ini meliputi 4 tahap rancangan skema jaringan, rancangan keamanan jaringan, rancangan aplikasi dan pengujian jaringan seperti dalam Gambar 1.



Gambar 1. Tahapan penelitian

2.2.1 Rancangan Skema Jaringan

Dalam tahap ini dilakukan perancangan skema jaringan pada PT Dae Myung Highness Indonesia. Hasil rancangan diperoleh topologi jaringan yang digunakan sehingga dapat dilakukan analisa kebutuhan yang diperlukan.

2.2.2 Rancangan Keamanan Jaringan

Dalam tahapan ini dilakukan rancangan keamanan jaringan PT Dae Myung Highness Indonesia sesuai yang dibutuhkan oleh perusahaan.

2.2.3 Rancangan Aplikasi

Pada tahap ini dilakukan perancangan aplikasi menggunakan *software* Ettercap pada Linux Backtrack dengan melakukan ARP *Poisoning* pada jaringan VPN. Untuk media komunikasi internal PT Dae Myung Highness Indonesia menggunakan *software openfire spark messenger*.

2.2.4 Pengujian Jaringan

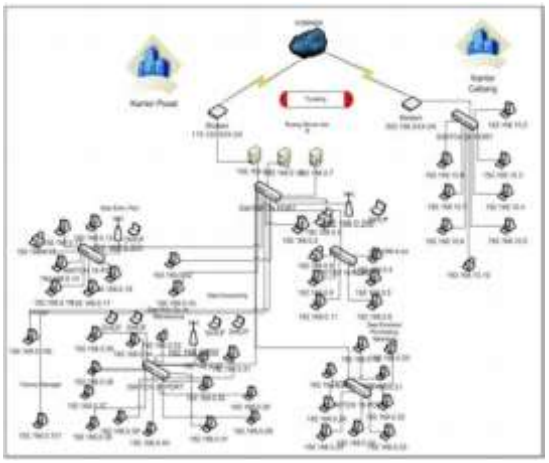
Dalam melakukan pengujian menggunakan *software packet tracer*. Pengujian dilakukan untuk mengetahui apakah perancangan yang telah dilakukan sudah memenuhi kebutuhan yang diharapkan.

3. Hasil dan Pembahasan

3.1. Skema Jaringan

Dalam implementasinya, untuk dapat menghubungkan antara kantor pusat dengan kantor cabang, pada masing-masing kantor membutuhkan sebuah *router* untuk membuat sebuah jaringan *virtual privat network*, dimana kantor pusat sebagai server dan kantor cabang sebagai *client.* Tahap konfigurasi VPN yang diusulkan adalah dengan membuat *tunneling* (PPTP) dan penerapan IP *security* untuk keamanan dalam pertukaran data.

Adapun konfigurasi jaringan usulan menggunakan *software* simulator dapat dilihat pada Gambar 2.



Gambar 2. Skema Jaringan Usulan

Tipe VPN yang di gunakan pada PT. Dae Myung Highness Indonesia adalah *remote access* VPN. *Remote access* VPN ini memberikan fasilitas bagi *user* untuk melakukan koneksi ke *server* VPN yang berada di LAN kantor cabang.

Dengan tipe seperti ini sebenarnya *user* VPN dapat mengakses *server* VPN dari mana saja selama ada koneksi internet, namun pada skripsi ini penulis melakukan implementasi *user* VPN hanya pada kantor PT. Dae Myung Highness Indonesia.

3.2. Keamanan Jaringan

Pada *router* mikrotik terdapat dua fitur yang ada di *firewall* yaitu *Network Address Translation* (NAT) dan *filter*.

1. Filtering

Keamanan jaringan dari aktivitas berbahaya dapat ditingkatkan dengan mengaktifkan PPTP *filtering* di *server* PPTP. Jika PPTP *filtering* diaktifkan, PPTP server di jaringan privat hanya akan menerima dan mengirim paket PPTP dari user yang terautentikasi. Dengan kata lain, mencegah semua paket lainnya untuk masuk ke dalam *server* PPTP dan jaringan privat. Bersama dengan pemakaian enkripsi PPTP, PPTP filtering menjaga agar hanya data yang terenkripsi dan terautorisasi yang dapat keluar masuk LAN privat perusahaan. PPTP *filtering* pada *server* PPTP dilakukan dengan men-setting Protocol di opsi *Network* dari *Control Panel*.

2. Network Address Translation

NAT merupakan salah satu protokol dalam suatu sistem jaringanVPN yang menggunakan *router* mikrotik. *Network Address translation* adalah fungsi *firewall* yang sebenarnya bertugas melakukan perubahan IP *address* pengirim dari sebuah paket data. NAT ini umumnya dijalankan pada router-router yang menjadi batas antara jaringan lokal dan jaringan internet. Secara teknis NAT ini akan mengubah paket data yang berasal dari komputer user seolah-olah berasal dari router. Router mikrotik nantinya akan menjalankan NAT dengan action=masquerade, sehingga mengubah semua paket data yang berasal komputer user seolah-olah berasal dari router. Marquerade ini wajib dijalankan oleh router-router gateway untuk menyembunyikan IP Address Private yang kita gunakan pada jaringan lokal, sehingga tidak terlihat dari internet. Masquerade tadi akan menyembunyikan komputer user yang ada dijaringan lokal sekaligus membuat komputer tersebut bertopeng ke IP Address router.

3.3. Rancangan Aplikasi

Untuk media komunikasi internal PT Dae Myung Highness Indonesia, penulis menggunakan *software openfire spark messenger* dengan terlebih dahulu *login* seperti pada Gambar 3.

Gambar 3. Login Spark Messenger

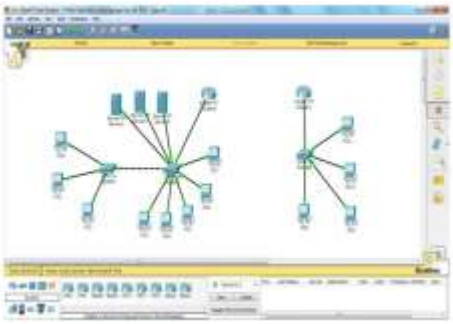
3.4. Pengujian Jaringan

Dalam melakukan pengujian jaringan penulis menggunakan software *packet tracer*. *Packet tracer* adalah

software buatan cisco yang digunakan untuk membuat jaringan komputer secara *virtual*, jadi tidak perlu takut jika terjadi *collision* atau tabrakan data yang bisa menyebabkan jaringan menjadi *down* dan akhirnya alat seperti *router* atau *switch* atau komputer bisa mengalami kerusakan.

3.4.1. Pengujian Jaringan Awal

Pengujian jaringan awal adalah pengujian jaringan yang sedang berjalan di PT. Dae Myung Highness Indonesia. Pengujian dilakukan dengan menggunakan *tools* buatan *cisco* yaitu *cisco packet tracer*. Pengujian ini akan meliputi pembuatan skema, pembagian *IP Static* untuk *server*, user dan tes koneksi baik dari *user* ke *server* ataupun tes koneksi antar *user*. Untuk di kantor cabang proses pengujian sama seperti di pusat karena jaringan di cabang berdiri sendiri dan tidak bisa terkoneksi dengan jaringan di pusat maka tes koneksi hanya akan melibatkan antar *user* di kantor cabang.

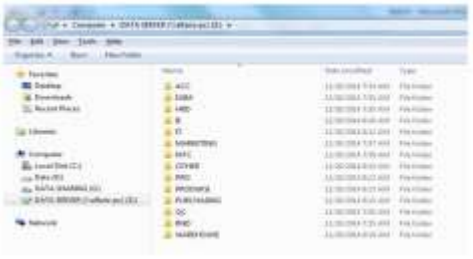


Gambar 4. Pengujian Jaringan Awal

3.4.2. Pengujian Jaringan Akhir

Pengujian jaringan akhir adalah pengujian rancangan jaringan usulan di PT. Dae Myung Highness Indonesia. Jaringan yang dirancang tidak jauh berbeda dengan jaringan yang sudah ada, komputer *user* dan komputer *server* juga tidak ada penambahan dan perubahan. Perubahan hanya terjadi pada pembuatan data *server* untuk memudahkan *user* berbagi *file* dan VPN *point to point tunneling protocol* yaitu terdapat sebuah lorong yang dapat diartikan bahwa proses tunneling adalah dengan membuat suatu tunnel di dalam jaringan publik untuk menghubungkan antara jaringan yang satu dan jaringan lain dari suatu grup atau perusahaan yang ingin membangun VPN (*Virtual Private Network*). Pertukaran data dan komunikasi jaringan akan melalui *tunnel* ini, sehingga orang atau *user* dari jaringan publik yang tidak memiliki izin untuk masuk akan sulit untuk menyadap data-data penting dalam jaringan. Berikut adalah tahapan instalasi data *server*:

1. Membuat folder pada *drive* yang dijadikan *server* atau *sharing* seperti dalam Gambar 5.



Gambar 5. Data Sharing Folder

2. *Setting permissions* pada user akses (*everyone*) kemudian pilih OK.
3. Pada user pilih run kemudian masukkan alamat *server* data. Setelah folder yang dilakukan *sharing* tampil kemudian *mapping* folder tersebut agar mudah diakses.

VPN *server* adalah suatu jaringan private yang menghubungkan jaringan satu dengan lainya melalui jaringan pribadi. Berikut adalah langkah-langkah instalasi dan pengujian VPN pada PT Dae Myung Highness Indonesia:

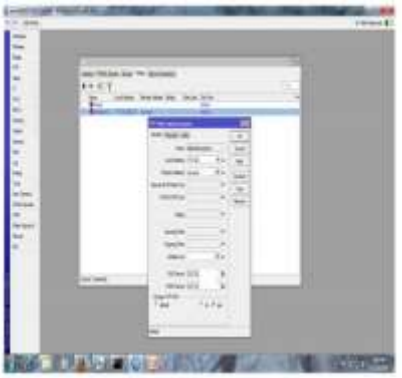
1. Buka *winbox* kemudian *login*. Pada menu pool isikan name kemudian isikan IP *address* untuk menentukan IP yang akan digunakan untuk VPN user.
2. Pada menu *pool* seperti pada Gambar 6 diisi pada name dan IP *address* untuk menentukan IP yang akan digunakan untuk VPN *user*.
3. Masuk ke menu ppp seperti pada Gambar 7 dan klik tanda plus lalu pilih pptp *server* kemudian isikan nama VPN yang akan dibuat seperti pada Gambar 8. setelah itu klik OK.
4. Pilih tab profiles seperti pada Gambar 9. dan isikan *local address* dengan IP *Public* VPN dan arahkan *remote address* ke IP *pool* yang telah dibuat sebelumnya.
5. Kemudian masuk ke tab *secret* seperti pada Gambar 10 dan buat name & password, isi *service* dengan pptp dan arahkan profile *default-encryption*.

Gambar 6. IP Pool

Gambar 7. Menu PPP

Form pengisian nama VPN.

Gambar 8. Interface Pptp Erp



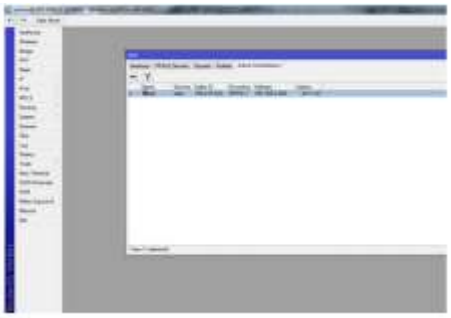
Gambar 9. Tab Profiles

Gambar 10. Tab Secrets

Setting VPN telah berhasil dan akan tampil pada *addres list* seperti pada Gambar 11.

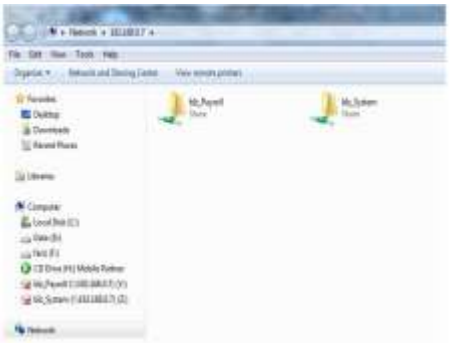
Gambar 11. Address List

Saat user terkoneksi dengan VPN server, akan tampil list user yang terkoneksi pada tab *active connections* di menu PPP seperti pada Gambar 12.



Gambar 12. Active Connections

File sharing via VPN sukses ditandai dengan tampilnya folder dari komputer yang dituju seperti pada Gambar 13.



Gambar 13. File Sharing Via VPN

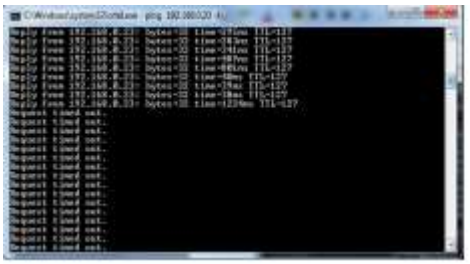
Selanjutkan akan dilakukan pengujian untuk mengakses ERP-SYSTEM via VPN dilakukan dengan terlebih dahulu buka aplikasi, masukan id dan *password* gambar 14. ERP-SYSTEM sukses diakses melalui VPN. Kemudian dilakukan pengetesan untuk mengoperasikan ERP-

SYS oba
mer ang
ada jian
mer ada
Gar

Gambar 14. Login Erp-System

Gambar 15. Modul Erp-System

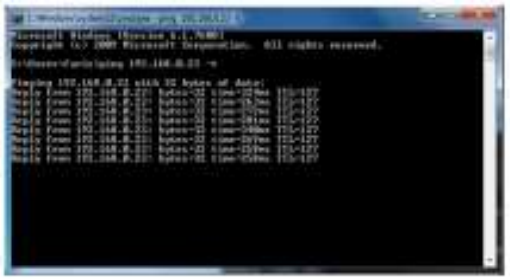
Pengujian serangan jaringan dilakukan dengan menggunakan metode D.O.S Pastikan jaringan sudah terkoneksi ke arah target, kemudian ketikan perintah "ping 192.168.0.23 (target)" Sebelum serangan dilakukan koneksi berjalan dengan normal seperti gambar 16.



Gambar 16. DOS

Kemudian ketikan perintah " ping 192.168.0.23 –t -l 65500" untuk mengaktifkan serangan ke target dan dapat

diperoleh jaringan target terputus seperti ditunjukan pada gambar 17.



Gambar 17. DOS Pingflood

Pengujian MITM dengan menggunakan Sistem Operasi Linux Backtraack, dengan Aplikasi ettercap dan Wireshark dilakukan dengan beberapa tahap:

1. Buka terminal baru lalu ketikan perintah "ettercap –G" seperti pada Gambar 18.

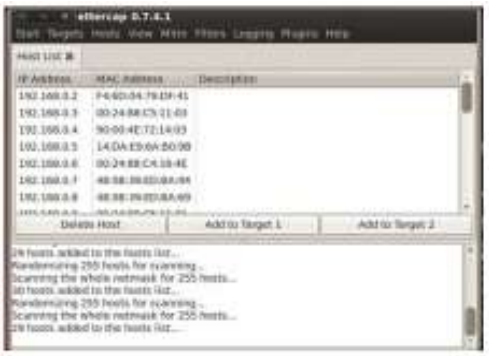
Gambar 18. Terminal Backtrack

Tampilan menu ettercap akan muncul dan pilih sniff > unified sniffing seperti Gambar 19.

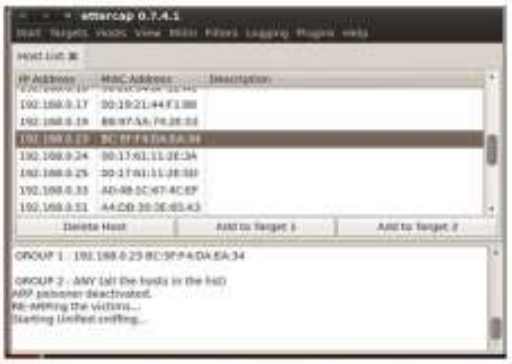
Gambar 19. Unified Sniffing

Host list akan tampil IP (*host*) yang berada dalam jaringan seperti pada Gambar 20.

2. *Starting Unified Sniffing* tampilan untuk target yang dituju seperti Gambar 21.
3. Buka aplikasi wireshark untuk mendapatkan pacet icmp dari target dan Pilih applications pada main menu > forensics > network forensics > wireshark seperti pada Gambar 22.



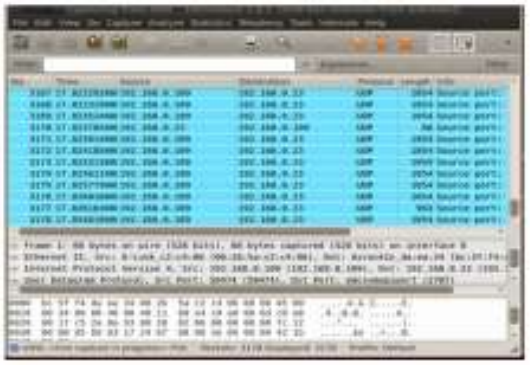
Gambar 20. Host List IP Address



Gambar 21. Starting Unified Sniffing

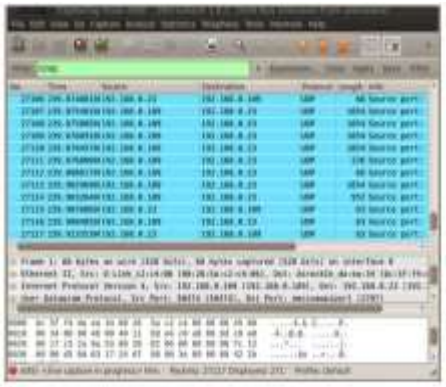
Gambar 22. Wireshark

Kemudian akan tampil packet data *active* pada target seperti pada Gambar 23.



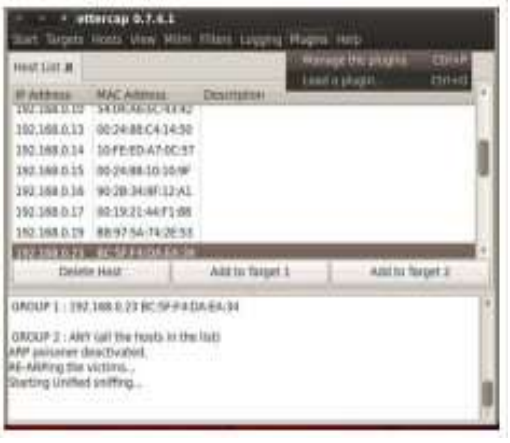
Gambar 23. Capturing From Eth0

Untuk melakukan monitoring *packet* icmp ketikan "icmp" pada kolom filter seperti pada Gambar 24.



Gambar 24. Monitoring Packet Filter "icmp"

Mematikan jaringan target kembali ke aplikasi *ettercap*, kemudian pilih menu *plugins* > *manage the plugins* seperti Gambar 25 dan muncul tampilan dns spoof seperti pada Gambar 26.



Gambar 25. Manage The Plugins

Gambar 26. Dns_spoof

4. Mengaktifkan jaringan target dengan memilih mitm > stop mitm attack(s) seperti pada Gambar 27.

Gambar 27. Stop Mitm Attack

Serangan pada target telah selesai dan akan tampil pemberitahuan *Man on the Middle* (MITM) *attack*(s) *stopped* seperti pada Gambar 28.

Gambar 28. Mitm Attack Stopped

4. Kesimpulan dan Saran

4.1. Kesimpulan

Kesimpulan yang dapat diambil yaitu:

1. Rancangan *Virtual Private Network* yang dilakukan sangat bergantung pada

kecepatan internet pada *server* maupun *user*, dan pada kasus yang ada di PT Dae Myung Highness Indonesia koneksi sudah cukup stabil untuk mengakses data *sharing server* dan ERP–SYSTEM maupun berkomunikasi dengan Spark Massenger.

2. Dari sisi keamanan jaringan pada VPN (*Virtual Private Network*) di PT Dae Myung Highness Indonesia cukup handal dalam menahan serangan dari luar jaringan PT Dae Myung Highness Indonesia.

4.2. Saran

Adapun saran-saran yang dapat diberikan kepada PT Dae Myung Highness Indonesia sebagai berikut:

1. Jika perusahaan ingin mengembangkan sistem jaringan di setiap kantor cabang sebaiknya menggunakan VPN dengan metode *site-to-site* sehingga koneksi VPN akan terjadi di masing-masing *router*. Dengan demikian akan memudahkan user dalam mengakses VPN karena *user* cukup memasukkan IP tujuan untuk dapat berkomunikasi tanpa harus memasukkan *username* dan password VPN *user.*
2. Perlu adanya pembenahan manajemen dan keamanan jaringan

Daftar Pustaka

Dodi Heriadi, 2012. Solusi Cerdas Menguasai Internetworking PACKET TRACER. Yogyakarta : Andi.

Hari Ratmoko1, Bowo Nurhadiyono 2012. Analisis Implementasi Keamanan Jaringan virtual Private Netword (VPN) Pada PT. LAYAR SENTOSA SHIPPING CORPORATION. Jurnal Vol. 2, no 1, Oktober 2012 (print).

I Nyoman Astawa Arya Gede, Atmaja Suta Dwi Ari I Made. 2012. Implementasi VPN Pada Jaringan Komputer Kampus Politeknik Negeri Bali. .Jurnal Matrix Vol 2 No 1 - Maret 2012 (print).

Putu Topan Pribadi, 2013. Implementasi HighAvailability VPN Client Pada Jaringan Komputer Fakultas Hukum Universitas UNDAYA. Bali.Jurnal Ilmu Komputer Vol 6-No 1 ISSN : 1979-5661 (Print).

Saputra, Andi. 2011 .Jenis-Jenis Mikrotik., [Serial Online]. http://unnes.info/informationtechnologies/jenis-jenis-mikrotik [Diakses pada 5 Desember 2014].

Sofana, Iwan. 2012.CISCO CCNP Jaringan Komputer. Bandung : Informatika

Towidjojo, Rendra. 2013. Mikrotik :Kitab 2. Jakarta :Jasakom.

Yoga Adyatma. 2012.Konfigurasi VPN PPTP pada Mikrotik. [Serial Online]. http://www.mikrotik.co.id/artikel_lihat.php?id=43 [Diakses pada 17 Desember 2014].