Analisis Keamanan Jaringan *Virtual Private Network* (VPN) pada Sistem *Online Microbanking*

Marti Widya Sari
Program Studi Teknik Informatika Fakultas Teknik
Universitas PGRI Yogyakarta
Jl. PGRI I No. 117 Sonosewu, Yogyakarta
mwidyas@gmail.com

Abstrak

Virtual Private Network (VPN), merupakan sebuah jaringan yang dibuat untuk melakukan transaksi data yang telah dienkripsi antara dua atau lebih pengguna jaringan yang resmi. Jaringan VPN seluruhnya menggunakan internet sehingga faktor keamanan menjadi sangat penting. Beberapa serangan yang mungkin terjadi di jaringan internet adalah *Denial of Service* (DoS) *attack*, *sniffing*, *spoofing*, *session hijacking*, dan masih banyak lagi.

Penelitian tentang analisis keamanan jaringan *Virtual Private Network* (VPN) ini dilakukan di BMT Al Ikhlas Yogyakarta, yang mempunyai sebuah kantor pusat dan beberapa kantor cabang serta menggunakan VPN untuk melakukan transaksi online antar cabang. Penelitian dilakukan dengan menggunakan metode *sniffing* (penyadapan) pada setiap paket yang melewati jaringan, kemudian melihat dan menganalisa hasilnya. Alat yang digunakan adalah *Wireshark Network Protocol Analyzer*. Penelitian dilakukan pada jaringan tanpa VPN, jaringan VPN Hamachi yang menggunakan teknologi IPSec (*IPSecure*) dan VPN Mikrotik yang menggunakan teknologi PPTP.

Abstract

Virtual Private Network (VPN), is a network created to conduct transactions encrypted data between two or more authorized network users. VPN network using the Internet so that all the safety factor becomes very important. Some of the attacks that may occur in the Internet network is a Denial of Service (DoS) attacks, sniffing, spoofing, session hijacking, and many more.

Research on the analysis of network security Virtual Private Network (VPN) is done in BMT Al Ikhlas Yogyakarta, which has a headquarters and several branch offices and use VPN to conduct online transactions between branches. Research carried out by using the method of sniffing (eavesdropping) on every packet that passes through the network, then view and analyze the results. The instrument used was the Wireshark Network Protocol Analyzer. The study was conducted on the network without a VPN, hamachi VPN using IPSec technology (IPSecure) and Mikrotik VPN using PPTP technology.

Keyword: VPN, VPN Hamachi, IPSec VPN, PPTP VPN

I. PENDAHULUAN

Penerapan teknologi informasi saat ini sudah menjadi kebutuhan semua pihak. Kebutuhan masyarakat untuk memberikan dan mendapatkan informasi secara cepat dan akurat sudah sangat tinggi. Informasi tersebut meliputi berbagai bidang, misalnya untuk bidang politik, ekonomi, sosial budaya, bidang perbankan dan juga bidang pendidikan. Selain itu, banyak perusahaan skala besar maupun kecil saat ini sudah menerapkan penggunaan aplikasi teknologi informasi dan internet, sehingga semua informasi tentang perusahaan dapat diketahui secara *online* dan *up to date*. Perusahaan yang mempunyai kantor pusat dan kantor cabang tentunya membutuhkan koneksi khusus agar tidak terganggu oleh pengguna lain dan meminimalkan adanya serangan keamanan komputer dari luar, salah satu caranya adalah dengan menggunakan *Virtual Private Network*. Menurut Forouzan (2007) VPN merupakan teknologi yang sangat populer digunakan oleh organisasi-organisasi besar dengan menggunakan sarana internet untuk berhubungan dengan intra atau antar organisasi untuk saling berkomunikasi tetapi membutuhkan *privacy* dalam berkomunikasi.

Lembaga keuangan mikro BMT Al Ikhlas saat ini sudah menggunakan koneksi *virtual private network* untuk menghubungkan kantor pusat dan cabang-cabangnya. VPN ini memudahkan komunikasi data antara kantor pusat dengan kantor cabang untuk menunjang transaksi *online banking*. Selain itu, penggunaan VPN ini tidak memerlukan biaya yang tinggi karena transmisi datanya menggunakan jaringan publik yang sudah ada yaitu internet. Jaringan VPN yang menggunakan jalur publik ini juga rentan terhadap serangan keamanan dari luar, misalnya *sniffing, spoofing, Denial of Service* (DoS), *Session Hijacking* dan lain-lain. VPN yang digunakan di BMT Al Ikhlas saat ini adalah jenis VPN Hamachi *free* atau tidak berbayar.

II. TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1 Tinjauan Pustaka

Pada tinjauan pustaka ini terdapat beberapa hasil penelitian yang dapat dijadikan referensi penelitian dan telah dipublikasikan melalui jurnal internasional.

Penelitian yang dilakukan oleh Alchaal, Roca dan Harbert (2004) tentang "*Managing and Securing Web Services with VPNs*". Layanan web merupakan satu set teknologi yang banyak dipercaya akan mengubah pandangan dalam komunikasi web untuk beberapa tahun mendatang. Layanan web menawarkan komunikasi standar dan mudah untuk sistem terdistribusi melalui internet. Namun sifatnya yang dinamis dan membutuhkan pengelolaan sistem secara baik, dan masalah keamanan menjadi kendala untuk penyebaran secara luas. Sementara itu ada kekhawatiran yang besar terhadap penggunaan VPN untuk mengamankan komunikasi di lingkungan yang hemat biaya seperti internet. Pada penelitian tersebut dijelaskan cara menggabungkan kedua teknologi dalam model hibrida baru yang kuat bahwa: 1) memungkinkan pengelolaan layanan web menjadi lebih, 2) menyediakan layanan web dengan penggunaan layanan keamanan VPN yang dinamis dan telah diprogram, dan 3) tetap sederhana dan terintegrasi. Pada penelitian tersebut dijelaskan juga tentang perbandingan teknologi SSL (*Secure Socket Layer*) dengan IPSec VPN.

Penelitian dilakukan oleh Hamed, Al-Shaer dan Marrero (2005) tentang "*Modelling and Verification of IPSec and VPN Security Policies*", yang melakukan

evaluasi tentang kegunaan dan performa dari IPSec pada jaringan VPN. IPSec telah menjadi sebuah protokol standar untuk keamanan komunikasi melalui internet, yang menyediakan layanan *integrity, confidentiality* dan *authentication*.

Penelitian yang dilakukan oleh Berger (2006) tentang "*Analysis of Current VPN Technology*", yang menjelaskan beberapa teknologi VPN yaitu IPSec (*IP Security*), L2TP (*Layer 2 Tunneling Protocol*) dan PPTP (*Point to Point Tunneling Protocol*). Pada penelitian tersebut juga dijelaskan mengenai kelebihan dan kekurangan menggunakan masing-masing teknologi tersebut, kelebihan dan kekurangan dari protokol-protokol tersebut sampai dengan analisis tentang interoperabilitas, pengaturan dan penerapan penanganan masalah yang ada.

Berdasarkan penelitian-penelitian tersebut, maka penelitian ini akan melakukan perbandingan untuk pengujian jaringan pada jaringan tanpa VPN, jaringan VPN dengan teknologi IPSec dan jaringan VPN menggunakan teknologi PPTP.

2.2 Landasan Teori

Definisi keamanan jaringan menurut Bastien dan Degu (2004) adalah implementasi perangkat keamanan, kebijakan dan proses untuk mencegah akses tanpa izin ke dalam sumber daya jaringan maupun melakukan perubahan atau kerusakan pada sumber daya atau data.

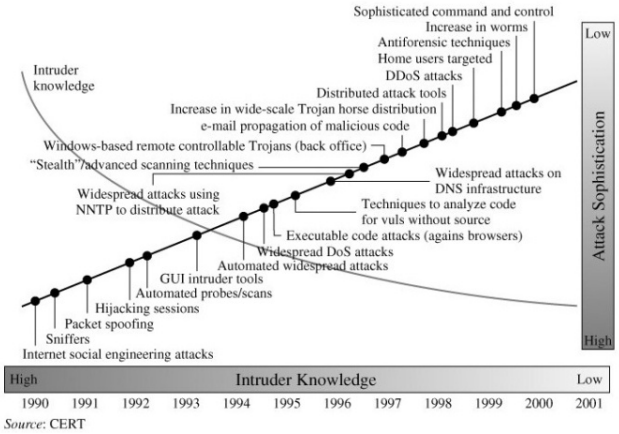
Menurut Garfinkel (2003), keamanan komputer (*computer security*) meliputi empat aspek yaitu *privacy and confidentiality, integrity, authentication dan availability.*

1. *Privacy and Confidentiality*
   Penjelasan dari aspek ini adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Privacy* lebih ke arah data-data yang sifatnya privat sedangkan *confidentiality* berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu.
2. *Integrity*
   Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seizin pemilik informasi tersebut. Contohnya adalah sebuah email dapat saja ditangkap (*intercept*) di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju. Penanggulangannya adalah dengan menggunakan enkripsi dan *digital signature*.
3. *Authentication*
   Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi benar-benar asli, orang yang mengakses atau memberikan informasi adalah benar-benar orang yang dimaksud, atau server yang dihubungi benar-benar server yang asli.
4. *Availability*
   Aspek ini berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang dapat menghambat atau meniadakan akses ke informasi.

2.2.1 Serangan Keamanan Jaringan

Serangan keamanan pada jaringan komputer maupun internet terjadi karena adanya kejahatan dunia maya (*cybercrime*). Jenis-jenis serangan keamanan yang mungkin terjadi misalnya adalah *spoofing, sniffing, phising, denial of service attack* (DoS), *brute force, SQL injection, session hijacking* dan masih banyak lagi. Pada Gambar 2.1 di bawah ini yang bersumber dari *Computer Emergency Response Team* (CERT) dan ditampilkan di buku "*Cryptography and Network Security"* oleh Stallings

(2005) menunjukkan serangan-serangan yang pernah terjadi mulai dari tahun 1990-2001 sesuai dengan tingkat pengetahuan penyerang (*intruder*).



Gambar 2.1 Trend kejahatan di dunia maya

a. *Denial of Service* (DoS) *Attack*
   Denial of Service Attack atau serangan DoS menurut Takanen, DeMott dan Miller (2008) adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber daya (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.
b. *Brute Force*
   Teknik *brute force* menurut Takanen, DeMott dan Miller (2008) merupakan teknik untuk mendapatkan informasi berupa *password* dengan cara menebak semua kemungkinan yang bisa didapatkan, misalnya dengan mencoba semua kata-kata yang umum digunakan atau memiliki relasi dengan pengguna yang ingin ditebak *password*nya.
c. *Session Hijacking*
   Session hijacking menurut Takanen, DeMott dan Miller (2008) merupakan tindakan pencurian session yang dilakukan oleh *remote user* untuk mendapatkan hak akses (*privilege*) ke sebuah sistem.
d. *SQL Injection*
   SQL injection menurut Clarke (2009) merupakan salah satu teknik dalam melakukan *web hacking* utk mendapatkan akses pada sistem *database* yang berbasis SQL. Teknik ini memanfaatkan kelemahan *scripting* pada SQL dalam mengolah suatu sistem *database*.

2.2.2 Virtual Private Network

Wide Area Netwok (WAN) digunakan untuk menghubungkan jaringan-jaringan lokal (LAN) satu dengan lainnya, baik yang berdekatan maupun berjauhan dan menggunakan protokol yang sama ataupun berbeda-beda. Jika pada LAN, jaringan komputer dapat dihubungkan menggunakan berbagai macam kabel, seperti: kabel koaksial, kabel UTP, serat optik, dan sebagainya, maka pada WAN pada umumnya

jaringan komputer dihubungkan melalui jaringan milik perusahaan telekomunikasi sebagai media perantara. Perusahaan telekomunikasi di Indonesia yang menyediakan sambungan untuk WAN antara lain: PT Telekomunikasi Indonesia, PT Indosat, PT Lintas Arta, PT Excelcomindo Pratama dan sebagainya. Menurut Wijaya (2004) terdapat beberapa teknologi yang dapat dipergunakan untuk menghubungkan WAN yaitu: *Dial Up*, *Leased Line*, VSAT, X.25, *Frame Relay*, *Virtual Private Network* (VPN), dan lain-lain. Pada penelitian ini akan dibahas tentang teknologi virtual private network yang digunakan untuk menghubungkan jaringan skala luas (WAN) pada BMT Al Ikhlas dan sistem keamanan jaringannya.

Menurut Forouzan (2007) VPN merupakan teknologi yang sangat populer digunakan oleh organisasi-organisasi besar dengan menggunakan sarana internet untuk berhubungan dengan intra atau antar organisasi untuk saling berkomunikasi tetapi membutuhkan *privacy* dalam berkomunikasi.

2.2.3 Standar Keamanan Jaringan VPN

Standar keamanan jaringan yang direkomendasikan pada Model Referensi OSI (CCITT, "*Security Architecture for Open System Interconnections for CCITT Applications*", CCITT, ITU CCITT X800, Geneva) adalah harus memenuhi persyaratan sebagai berikut :

1. *Authentication Service*
   VPN *Service Provider* tidak dapat menyimpan seluruh identitas informasi yang dimilik oleh seluruh pengguna (*end-user*). Pada konteks VPN, hal ini akan termasuk dalam layanan autentikasi pengguna yaitu layanan autentikasi pelanggan dan layanan autentikasi keaslian data. Sebagai contoh: seorang pengguna dapat memanfaatkan layanan yang disediakan oleh *vendor* dan akan dikontrol melalui sebuah mekanisme autentikasi, seperti penggunaan *password*.
2. *Access Control*
   Access Control pada layanan VPN sangat diperlukan untuk memfilter/menyaring akses koneksi VPN ke operasional manajemen maupun ke pelanggan dan direktori pribadi.
3. *Data Integrity and Confidentiality*
   Layanan ini berfungsi untuk melindungi data pada VPN dari serangan oleh pihak yang tidak berwenang dan ancaman dari luar. Ancaman ini dapat berupa modifikasi, menambah maupun menghapus informasi pada manajemen.

2.2.4 Microbanking

Microbanking atau sering disebut dengan *microfinance* adalah sebuah lembaga keuangan mikro yang mempunyai segmentasi pasar menengah ke bawah terutama bagi pengusaha kecil maupun masyarakat yang kesulitan mendapatkan akses pinjaman ke bank. Contoh *microbanking* yang dikenal di Indonesia adalah Bank Perkreditan Rakyat/Syariah (BPR/BPRS), *Baitul Maal watTamwil* (BMT) yang mempunyai badan hukum sebagai koperasi, Koperasi Serba Usaha (KSU), Koperasi Simpan Pinjam (KSP) dan sebagainya.

Saat ini tidak hanya bank-bank besar atau bank umum nasional saja yang dituntut untuk menggunakan teknologi informasi sebagai bagian dari proses bisnis yang

ada, tetapi *microbanking* juga sudah mulai memanfaatkan penggunaan teknologi informasi untuk melayani nasabahnya. Hal ini dapat dilihat dari penggunaan aplikasi sistem informasi akuntansi untuk melakukan layanan maupun pencatatan transaksi, jadi sudah meninggalkan sistem manual, walaupun belum seluruhnya memanfaatkan teknologi informasi ini.

IV. METODOLOGI PENELITIAN

Pada bab ini diuraikan tentang detail cara penelitian, yaitu sebagai berikut:

3.1 Bahan Penelitian

Semua bahan dan materi yang ada pada penelitian keamanan jaringan *virtual private network* (VPN) ini merupakan hasil dari suatu proses implementasi yang telah digunakan oleh instansi yang bersangkutan.

3.2 Alat Penelitian

Alat yang digunakan dalam penelitian ini adalah menggunakan komputer dengan spesifikasi cukup untuk menjalankan *software* aplikasi *virtual private network* di atas sistem operasi Windows. Software aplikasi VPN yang digunakan adalah Hamachi™ dari *vendor* LogMeIn®.

3.3 Metode Penelitian

Metode penelitian yang dilakukan meliputi survey ke lokasi penelitian, identifikasi masalah, mengumpulkan data, studi kepustakaan, analisa data kemudian membuat rekomendasi dari hasil penelitian yang dilakukan.

3.3.1 Melakukan Survey ke Lokasi Penelitian

Salah satu jalan penelitian adalah melakukan survey langsung ke instansi tempat dilakukan penelitian yaitu di BMT Al Ikhlas pusat.

3.3.2 Identifikasi Masalah

Pada penelitian ini dilakukan identifikasi masalah yang menjadi obyek penelitian. Masalah-masalah yang terjadi selama menggunakan VPN adalah sebagai berikut :

1. VPN yang digunakan berbasis *software* (*software based*) yaitu dengan menggunakan *software* Hamachi versi 1.0.3.0. VPN yang digunakan saat ini kadang-kadang mengalami masalah koneksi, misalnya tiba-tiba koneksi terputus, baik disebabkan oleh putusnya jaringan internet maupun tidak dapat terhubung ke server Hamachi.
2. Koneksi VPN ini hanya digunakan untuk mendukung transaksi online menggunakan sistem informasi akuntansi *Integrated microBanking System*.
3. Kemudian dibuat koneksi VPN menggunakan PPTP VPN server Mikrotik sebagai cadangan jika koneksi VPN menggunakan Hamachi sedang mati.

3.3.3 Mengumpulkan Data

Pengumpulan data dilakukan melalui observasi langsung ke lokasi penelitian dan wawancara dengan administrator selaku penanggung jawab operasional IT secara *personal interview* yaitu bertatap muka secara langsung. Data yang terkumpul berupa permasalahan yang terjadi selama menggunakan VPN, teknologi VPN yang digunakan saat ini, software dan hardware pendukung yang digunakan serta hasil dari pengujian sistem yang saat ini digunakan.

3.3.4 Studi Kepustakaan

Studi kepustakaan dilakukan untuk mencari literature yang berhubungan dengan obyek penelitian ini, serta untuk memahami konsep tentang *virtual private network*. Selain itu, juga terdapat buku, jurnal ilmiah artikel, artikel di internet dan sebagainya.

3.3.5 Analisa Data

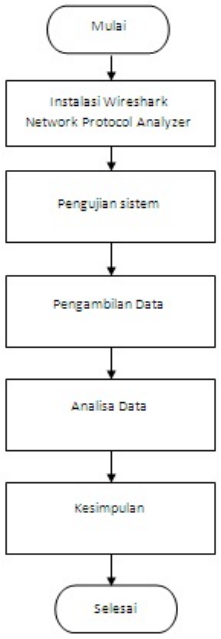
Setelah data terkumpul, maka dilakukan analisa terhadap keseluruhan data yang sudah diperoleh. Analisa data yang dilakukan adalah dengan melihat hasil penelitian yang ada, yaitu hasil pengujian untuk jaringan yang tidak menggunakan koneksi VPN, kemudian hasil pengujian untuk jaringan yang menggunakan koneksi VPN, dan koneksi VPN menggunakan *dial* VPN dengan teknologi PPTP.

3.3.6 Membuat Rekomendasi tentang Hasil Penelitian

Rekomendasi atau usulan dibuat berdasarkan observasi di lokasi penelitian, wawancara dengan administrator maupun melalui analisa data.

3.4 Flowchart Penelitian

Penelitian akan dilakukan melalui dua tahap, yaitu pertama, menguji sistem yang tidak menggunakan VPN dan kedua, menguji sistem yang menggunakan VPN.



Gambar 3.1 Flowchart Penelitian

Flowchart di atas menunjukkan lanngkah-langkah yang akan dilakukan untuk pengujian sistem menggunakan tools *Wireshark Protocol Analysis*.

IV. HASIL PENELITIAN DAN PEMBAHASAN

Pada penelitian ini terdapat dua jenis jaringan komputer yaitu yang tidak menggunakan VPN dan yang menggunakan VPN, serta dilakuakn pengujian untuk kedua macam jaringan tersebut. Hal ini disebabkan di BMT Al Ikhlas tidak semuanya terkoneksi dengan jaringan VPN. Jaringan di kantor pusat menggunakan jaringan lokal

(LAN) yang terkoneksi dengan internet, sedangkan untuk berhubungan antara kantor pusat dengan kantor cabang menggunakan jaringan VPN dengan *software* Hamachi.

4.1 Jaringan *Existing* di Lokasi Penelitian

Pada penelitian ini terdapat dua jenis jaringan komputer yaitu yang tidak menggunakan VPN dan yang menggunakan VPN, serta dilakukan pengujian untuk kedua macam jaringan tersebut. Hal ini disebabkan di BMT Al Ikhlas tidak semuanya terkoneksi dengan jaringan VPN. Jaringan di kantor pusat menggunakan jaringan lokal (LAN) yang terkoneksi dengan internet, sedangkan untuk berhubungan antara kantor pusat dengan kantor cabang menggunakan jaringan VPN dengan *software* Hamachi.

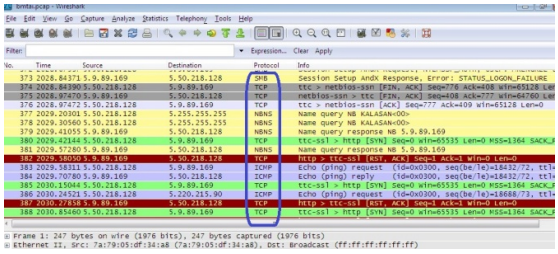
Jaringan VPN ini menggunakan *software* Hamachi dari *vendor* LogMeIn. Penggunaan software Hamachi dipilih karena kemudahan dalam instalasi dan setingnya. Selain itu, Hamachi juga menyediakan fasilitas yang mendukung keamanan jaringan VPN seperti untuk autentikasi dan enkripsi. VPN yang digunakan disini termasuk *software based*, karena menggunakan *software* untuk membuat koneksi VPN. *Software* Hamachi yang digunakan adalah versi 1.0.3.0.

4.2 Pengujian pada Jaringan

Pada penelitian ini dilakukan pengujian pada tiga konfigurasi jaringan, yaitu: pada jaringan tanpa VPN, pengujian pada jaringan yang menggunakan VPN Hamachi dan pada jaringan yang menggunakan PPTP VPN.

4.2.1 Pengujian pada Jaringan Tanpa VPN

Software Wireshark dipasang di antara server dan *client* lalu menangkap setiap paket yang melewati jaringan keduanya. Selain itu akan dianalisis isi dari paket tersebut untuk menganalisa celah keamanan lainnya. Skenario yang dibuat adalah server dan client akan berkomunikasi dan client mengirimkan data ke server. Kemudian data yang lewat akan di*sniffing* oleh Wireshark. Hasil dari *sniffing* akan terlihat data yang dikirimkan dari client ke server. Dari analisis di atas dapat diketahui celah keamanan jaringan pada saat pengiriman data.

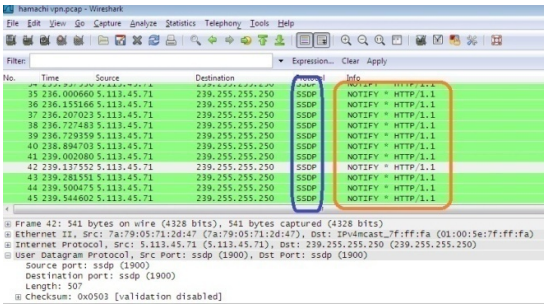


Gambar 4.1 Hasil pengujian pada jaringan tanpa VPN

Hasil *sniffing* pada Gambar 4.1 memperlihatkan terdapat beberapa protokol yang tertangkap yaitu: SMB, TCP, NBNS dan ICMP. *Source* menunjukkan alamat asal atau sumber sedangkan *Destination* menunjukkan alamat yang dituju.

4.2.2 Pengujian pada Jaringan VPN Hamachi

Pada pengujian sistem yang menggunakan VPN ini dilakukan dengan metode *sniffing*, yaitu menangkap setiap paket yang melewati antara server dan client dalam jaringan VPN.

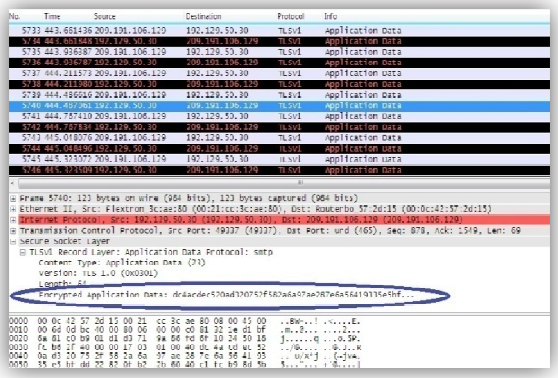


Gambar 4.2 Hasil pengujian pada jaringan VPN Hamachi

Pada hasil pengujian sistem jaringan VPN, Gambar 4.2, tidak dapt dilihat informasi pertukaran data yang dilakukan antara server dan client. Selain itu yang muncul adalah protokol SSDP (*Simple Service Dicovery Protocol*). Protokol SSDP dapat menemukan perangkat *Plug & Play*, dengan UPnP (*Universal Plug and Play*). SSDP menggunakan alamat *unicast* dan *multicast* (239.255.255.250). SSDP adalah seperti protokol HTTP (*Hypertext Transfer Protocol*) dan bekerja dengan metode NOTIFY dan M-SEARCH. SSDP menggunakan metode NOTIFY HTTP untuk mengumumkan pembentukan atau penarikan informasi ke grup *multicast*.

4.2.3 Pengujian pada Jaringan PPTP VPN

Pengujian untuk jaringan VPN juga dilakukan pada jaringan VPN PPTP menggunakan router Mikrotik. Hal ini dilakukan dengan cara melakukan *sniffing* dari luar jaringan VPN PPTP yang ada.



Gambar 4.3 Hasil pengujian pada jaringan PPTP VPN

Pada pengujian ini, komputer yang berada di kantor cabang mencoba melakukan koneksi ke alamat IP 209.191.106.129. Sedangkan pada kolom protokol yang terlihat adalah protokol TLSv1 (*Transport Layer Security* version1.0), seperti pada Gambar 4.3.

TLS merupakan bagian dari protokol SSL (*Secure Socket Layer*), dan pada keterangan dapat dilihat bahwa data terenkripsi (*Encrypted Application Data*).

4.3 Rekomendasi

Dari hasil penelitian di atas, maka dapat diuraikan beberapa rekomendasi untuk hal *software, hardware* maupun dokumentasi seperti berikut:

1. Software hamachi VPN yang digunakan saat ini sudah mendukung teknologi IPSecure (IPSec) yang mempunyai standar keamanan tinggi seperti yang direkomendasikan pada Model Referensi OSI (CCITT, "*Security Architecture for Open System Interconnections for CCITT Applications*", CCITT, ITU CCITT X800, Geneva). Tetapi terdapat sebuah kendala yang perlu dipertimbangkan, yaitu dengan menggunakan software Hamachi ini berarti dalam proses transmisi data, semua data sebelum sampai ke tujuan akan dilewatkan dahulu ke server mediasi miliki vendor LogMeIn, kemudian baru diteruskan ke *node* tujuan. Sementara data-data yang diakses dan dikirimkan melalui VPN tersebut merupakan data-data penting yang menyangkut transaksi keuangan. Selain itu, pengguna software Hamachi ini juga tidak dapat mengelola server sendiri, karena tidak ada hak untuk mengakses server. Hal ini yang harus dipertimbangkan kembali.
2. Penggunaan teknologi VPN pada Mikrotik perlu dimaksimalkan, karena pada router Mikrotik sudah mendukung penggunaan teknologi *IPSecure* (IPSec), sedangkan yang digunakan saat ini adalah PPTP VPN. Teknologi PPTP ini sendiri sudah cukup aman, tetapi jika diinginkan keamanan dengan standar tinggi dapat digunakan teknologi IPSec menggunakan router Mikrotik. Penggunaan PPTP ini dapat digunakan sebagai koneksi VPN utama. Karena dengan koneksi ini, administrator dapat mengelola server maupun jaringan VPN secara mandiri.
3. Penggunaan hardware yang dapat meningkatkan performa keamanan jaringan adalah penggunaan hub dalam konfigurasi jaringan yang digunakan saat ini kurang tepat, dan dapat diganti menggunakan Switch untuk meningkatkan performa jaringan lokal (LAN).
4. Penggunaan Router Mikrotik RB750 sudah cukup memadai, namun jika diinginkan untuk tingkat keamanan lebih lanjut dapat digunakan hardware yang sudah mendukung *built-in encryption engine* dan menggunakan teknologi IPSec, seperti: Mikrotik Router Board RB 1000, RB 1100AH maupun RB 1200.
5. Perlu dibuat dokumentasi secara lengkap dalam hal:
   a) Dokumentasi untuk memonitor dan membuat laporan secara berkala untuk keadaan jaringan. Melakukan monitoring terhadap keadaan jaringan serta membuat laporan keadaan jaringan agar dapat digunakan sebagai acuan di masa yang akan datang. Hal ini sangat penting mengingat setiap saat terdapat perubahan trafik maupun performa jaringan.
   b) *Standar Operating Procedure* (SOP) untuk operasional IT untuk mendukung pemanfaatan jaringan secara opetimal. SOP akan sangat berguna sebagai acuan standar dalam mengelola jaringan maupun IT secara keseluruhan.

V. KESIMPULAN DAN SARAN

Pada pokok bahasan IV telah diuraikan mengenai hasil-hasil penelitian beserta pembahasannya. Hasil akhir dari penelitian ini adalah berupa rekomendasi yang

nantinya dapat berguna bagi perbaikan keamanan jaringan instansi yang bersangkutan di masa mendatang.

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penelitian ini adalah:

1. Hasil penelitian menunjukkan bahwa sistem yang tidak menggunakan VPN lebih rentan. Hal ini dapat dilihat dari paket-paket yang ditangkap, pada jaringan tanpa menggunakan VPN datanya tidak terenkripsi, jadi mudah diambil maupun dimanfaatkan oleh pihak lain. Seperti terlihat pada hasil pengujian, protokol-protokol yang muncul antara lain SMB, NBNS, ICMP dan TCP, serta muncul informasi tentang transaksi data yang sedang terjadi.
2. Pengujian antara koneksi VPN menggunakan Hamachi dan VPN menggunakan PPTP menunjukkan hasil yang berbeda. Pada pengujian VPN Hamachi yang muncul adalah protokol SSDP (*Simple Service Discovery Protocol*) dengan metode Notify, sedangkan pada pengujian menggunakan PPTP VPN, protokol yang muncul adalah TLSv1 (*Transport Layer Security version* 1.0) yang merupakan pembaharuan dari SSL (*Secure Socket Layer*). Pada pengujian kedua koneksi VPN tersebut tidak dapat dilihat transaksi data yang sedang dilakukan di jaringan itu. Jadi pada sistem yang menggunakan VPN, datanya terenkripsi sehingga lebih aman karena tidak dapat dilihat oleh pihak lain.
3. Router Mikrotik RB750 tidak hanya mendukung teknologi PPTP tetapi juga sudah mendukung teknologi IPSec VPN.
4. Setiap node LogMeIn Hamachi memiliki pilihan administratif untuk membantu menjaga keamanan jaringan Hamachi, yaitu dengan adanya fasilitas: *Password Protection, Network Lock, Membership Approval, Membership Eviction/Ban.*
5. Penggunaan teknologi VPN Hamachi pada sistem *online microbanking* ini sangat membantu dalam melakukan transaksi antar kantor cabang. Selain itu teknologi VPN ini juga memberikan keamanan pada transmisi datanya, tetapi mekanisme koneksi VPN pada Hamachi ini yang mempunyai kekurangan, yaitu semua data yang lewat harus melalui server mediasi atau server antara yang berada di sisi vendor LogMeIn dan tidak dapat dikelola secara mandiri.

5.2 Saran

Saran-saran yang dapat penulis uraikan adalah sebagai berikut:

1. Perlu dibuat *Standar Operating Procedure* (SOP) dan dokumentasi yang lengkap untuk operasional IT di BMT Al Ikhlas. SOP ini akan sangat berguna untuk penggunaan serta pemanfaatan jaringan secara optimal, selain itu dapat bermanfaat jika ada penelitian selanjutnya.
2. VPN dapat dimanfaatkan untuk pertukaran file maupun data, karena di BMT Al Ikhlas jaringan VPN yang ada hanya digunakan untuk menghubungkan aplikasi sistem informasi akuntansi IBSS.
3. Teknologi VPN yang saat ini digunakan untuk sistem *online microbanking* yaitu Hamachi, mempunyai mekanisme koneksi yang kurang menguntungkan bagi para penggunanya dan tidak dapat dapat dikelola secara mandiri, maka alternatif yang dapat diberikan adalah dengan mengganti koneksi menggunakan peralatan yang sudah ada yaitu router Mikrotik dengan teknologi PPTP.

4. Untuk penelitian di masa mendatang dapat dilakukan dengan meneliti tentang performa jaringan, melakukan optimalisasi konfigurasi jaringan serta melakukan *benchmarking* untuk jaringan VPN yang ada.

DAFTAR PUSTAKA

[1] Bastien, G; Degu, C.A. 2004. *CCSP Secure Exam Certification Guide.* Cisco Press. Indianapolis, USA

[2] Berger, T. 2006. *Analysis of Current VPN Technologies*. IEEE Journal.

[3] Brown, L. 2003. *Lecture Notes for Use with Cryptography and Network Security by Willliam Stallings*.

[4] Clarke, J. 2009. *SQL Injection Attack and Defense*. Syngress Publishing, Inc., Elsevier, Inc. Burlington, MA.

[5] Forouzan, B.A. 2006. *TCP/IP Protocol Suite (Third Edition)*. McGraw-Hill Companies, Inc. New York.

[6] Garfinkel, S; Spafford, G; Schwartz, A. 2003. *Practical UNIX and Internet Security (Third Edition)*. O'Reilly & Associate Inc. Sebastopol, CA.

[7] Hamed, H; Al-Shaer, E; Marrero, W. 2005. *Modelling and Verification of IPSec and VPN Security Policies*. IEEE Journal.

[8] Held, G. 2003. *Securing Wireless LANs: A Practical Guide for Network Managers, LAN Administrators and the Home Office User*. John Wiley & Sons Ltd. West Sussex, England.

[9] Held, G. 2004. *Virtual Private Networking: A Construction, Operation and Utilization Guide*. John Wiley & Sons Ltd. West Sussex, England.

[10] Kaeo, M. 2003. *Designing Network Security 2nd Edition*. Cisco Press. Indianapolis, USA.

[11] Lewis, E; Davies, J. 2003. *Deploying Virtual Private Networks with Microsoft Windows Server 2003*. Microsoft Press. Redmond.

[12] Lewis, M. 2006. *Comparing, Designing and Deploying VPNs*. Cisco Press. Indianapolis. USA

[13] McNab, C. 2008. *Network Security Assessment, Second Edition*. O'Reilly Media, Inc. Sebastopol, CA.

[14] Mathison, S. *Increasing the Outreach and Sustainability of Microfinance through ICT Innovation*, The Foundation for Development Cooperation (FDC).

[15] Schneier, B; Mudge. *Cryptanalysis of Microsoft's PPTP*. Mountain View. CA.

[16] Stallings, W. 2005. *Cryptography and Network Security Principles and Practices, Fourth Edition*, Prentice-Hall, New Jersey.

[17] Stiawan, D. 2003. *Perancangan Sistem Virtual Private Network (VPN) Pada Jaringan Skala Luas (WAN) Studi Kasus di PT Pupuk Sriwidjaja Palembang.* Tesis tidak terpublikasi. Yogyakarta : Universitas Gadjah Mada.

[18] Takanen, A; DeMott J; Miller C. 2008. *Fuzzing for Software Security Series Testing and Quality Assurance*. Artech House, Inc. Canton Street, Norwood, MA.

[19] Tellen, S. 2005. *Intranet Organization: Strategies for Managing Change*.

[20] Versalone, J. 2008. *Microsoft Forefront Security Administration Guide*. Syngress Publishing, Inc. USA.