ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN VPN RADUIS (REMOTE AUTHENTICATION DIAL-IN USER SERVICE) PADA JARINGAN WIRED LAN (THE IMPLEMENTATION AND ANALYSYS VPN RADIUS (REMOTE AUTHENTICATION DIAL-IN USER SERVICE) SECURITY SYSTEM IN WIRED LAN NETWORK)

Muhammd Imron[1], R. Rumani[2], Akhmad Hambali[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

RADIUS merupakan sistem keamanan yang berbasis AAA (Authentication, Authorization, Accounting) yang sudah tergabung didalamnya. Dengan mekanisme tersebut mengurangi kebutuhan dukungan administratif dan meningkatkan keamanan jaringan. RADIUS bekerja pada sistem operasi FreeBSD-6.3 STABLE. Sistem ini dibangun oleh sistem utama yakni VPN service berjalan diatas jaringan IPv4 yang didalamnya terdapat beberapa service diantaranya database server, radius server, pptp server, dan proxy server. Semua service tersebut sudah ter-install dalam satu komputer sehingga sistem menjadi lebih efisien.

Dalam implementasi kali ini ada beberapa tools yang dipakai yakni: hardware (sebuah komputer sebagai server, sebuah switch 24 port), software (FreeBSD-6.3 STABLE, Poptop -1.3.4_1, FreeRADIUS-1.1.7_3, Apache HTTPd, MySQL-5.0.51a, ALTQ, SQUID). Sedangkan tools sebagai untuk mengambil parameter yakni: Packet sniffer, NTP server, Putty, dan wireshark.

Ada beberapa parameter yang diambil pada RADIUS server yakni: latency, sistem keamanannya, delay, throughput, time login. Parameter latency diambil sebagai dasar dalam pengambilan parameter lainnya. Latency pada jaringan VPN RADIUS mempunyai nilai lebih kecil dibandingkan jaringan biasa, hal ini karena proses enkapsulasi paket sebelum dikirim. Kedua parameter delay pada jaringan VPN RADIUS mempunyai nilai lebih besar dibandingkan jaringan biasa, hal ini karena proses AAA (Authentication, Authorization, Accounting). Ketiga parameter throughput pada jaringan VPN RADIUS mempunyai nilai lebih kecil dibandingkan jaringan biasa, hal ini karena proses enkapsulasi menjadikan panjang paket pada VPN RADIUS menjadi lebih besar. Keempat time login, untuk beberapa panjang karakter username dan password yang berbeda menghasilkan nilai time login yang berbeda pula, namun panjang karakter tidak mempengaruhi time login. Hal ini karena time login tidak terpengaruh panjang karakter tetapi dipengaruhi latency jaringan. Semakin bersar latency semakin lama time login.

Kata Kunci : AAA, IPv4, keamanan, RADIUS, VPN

Abstract
RADIUS is an security system based on AAA (Authentication, Authorization, Accounting) which is tergabung inside it. With this mechanism, administrative support can be reduced and can increase the network security. RADIUS work on FreeBSD-6.3 STABLE Operating System. This system is built with main system, that is VPN service and work on IPv4 network which have several services inside it, there are database server, radius server, pptp server, dan proxy server. All of this service has been installed in a co,puter so the system is more efficient.

In this implementation there are several tools which is used, there are : hardware (a computer as server, a 24 port switch), software (FreeBSD-6.3 STABLE, Poptop -1.3.4_1, FreeRADIUS-1.1.7_3, Apache HTTPd, MySQL-5.0.51a, ALTQ, SQUID). And tools as parameter gained is Packet sniffer, NTP server, Putty, dan wireshark.

Therearte several parameters which is taken to RADIUS server, there are: latency, security system, delay, throughput, tiome login. Latency parameter is taken as dasar in another parameter. Latency in VPN RADIUS network is smaller than ordinary network because encapsulation package proccess before the package is sent. Second, delay parameter in VPN RADIUS network is bigger than ordinary network, because the AAA (Authentication, Authorization, Accounting) proccess. Third, throughput parameter in VPN RADIUS network is smaller than ordinary network because encapsulation proccess make packages of VPN Radius more bigger. Fourth, time login, for some different username and password do not influence the time login. This is because time login do not have any relationship with the number of character but influenced by network‟s latency. More latency means more time login.

Keywords : AAA, IPv4, security, RADIUS, VPN

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Penggunaan *internet* saat ini sangat dibutuhkan diberbagai bidang seperti pendidikan, kesehatan, informasi, bisnis, militer dan bidang lainnya. Keberadaan *internet* sangat memudahkan para pengguna layanan ini untuk melakukan berbagai macam kegiatan antara lain transaksi secara *online, internet banking*, *email*, dan lain-lain.

Pengguna *internet* yang semakin bertambah tentu membutuhkan suatu sistem management *user* yang handal. Suatu sistem yang mampu melakukan proses registrasi (*authentication* dan *authorization*) *user*, *accounting* secara *realtime*, *bandwidth management* untuk tiap-tiap tingkatan *user*. Selain proses *authentikasi – authorisasi – accounting*, *bandwidth management*, dibutuhkan juga sebuah komunikasi data yang aman antara *client* ke *client*, maupun dari *client* ke *internet gateway* (*proxy*). Komunikasi data yang aman dapat dilakukan dengan menggunakan *Virtual Private Networks* (VPN). VPN menjadi satu solusi yang tepat dalam menjamin kemananan data baik antara *client* ke *client* dan *client* ke *internet gateway*. Dengan VPN, proses trafik data tidak dapat disadap dengan mudah oleh pihak lain.

Dalam Tugas Akhir ini, akan dibuat sebuah sistem *management internet user* dengan menggunakan VPN sebagai *backend* jaringannya beserta analisis dari sistem, RADIUS untuk proses *management user* (*Authentication, Authorization, Accounting*) dan ALTQ untuk *bandwidth management* sistemnya. Hasil akhirnya adalah sebuah sistem *internet management user* yang mendukung ketiga servis diatas beserta anlisis parameternya.

1.2 Tujuan

Tujuan dari penelitian yang akan dilakukan yaitu meliputi :

1. Membuat sistem keamanan yang tingkat keamanan yang tinggi dan efisien.
2. Memberikan kemudahan administrator sebagai penyelenggara Wired LAN dalam memanajemen dan memonitoring serta mengontrol *bandwidth* dalam jaringan.

3. Menganalisa apakah terdapat celah keamanan pada sistem keamanan jaringan dengan menggunakan RADIUS *server*.
4. Memberikan kemudahan antar *remote side* untuk bisa mengakses RADIUS *server* secara aman.
5. Menghasilkan sebuah sistem *internet* manajemen *user* yang berbasiskan VPN dan RADIUS.

1.3 Perumusan Masalah

Pada Tugas Akhir ini dirumuskan masalah sebagai berikut :

1. Bagaimana cara instalasi RADIUS *server* dalam sistem operasi FreeBSD-6.3 STABLE.
2. Mekanisme pembatasan *bandwith* dengan menggunakan algoritma HSFC (*Hierarchical Fair Service Curve*).
3. Bagaimana caranya melakukan *hack* ke jaringan keamanan RADIUS (teknik, peralatan).
4. Menganalisa kinerja (QoS) dari sistem RADIUS *server*.
5. Menginstal, mengkonfigurasi *Apache* dengan modul PHP dan MySQL sebagai perangkat lunak portal dan *database*.
6. Bagaimana mengkonfigurasi ALTQ (*Alternate Queuing*) merupakan aplikasi yang digunakan untuk *packet scheduling* dikombinasikan dengan *Packet Filter* (PF) dan menghasilkan sebuah *firewall* dan *packet scheduling*. ALTQ diterapkan di sisi *server*.

1.4 Batasan Masalah

Ruang lingkup dalam pembahasan Tugas Akhir ini adalah sebagai berikut :

1. Sistem berjalan diatas sistem operasi FreeBSD.
2. Protokol yang digunakan adalah protokol PPTP.
3. Jaringan berjalan di jaringan IPv4
4. Komputer sebagai *client* dengan OS Windows XP2
5. Teknik, peralatan (keras maupun lunak) *hacking*.

1.5 Metodologi Penelitian

Metode penelitian yang digunakan dalam penyelesaian Tugas Akhir ini akan dilakukan secara bertahap. Tahapan tersebut adalah sebagai berikut :

1. **Studi literatur**

   Studi literatur dilakukan dengan mengumpulkan konsep yang digunakan dalam pemodelan melalui referensi. Referensi tersebut bisa didapatkan melalui buku–buku referensi, informasi dari internet, diskusi dengan pembimbing serta pihak–pihak yang mempunyai pengetahuan dan pengalaman mengenai sistem keamanan dengan RADIUS server.

2. **Pembuatan sistem yang siap untuk kegiatan *hacking***

   Meliputi tahapan terstruktur sebagai berikut :

   1. Perancangan sistem yang dimaksudkan, meliputi kelengkapan perangkat keras dan lunaknya.
   2. Implementasi dan Uji Coba.

3. **Studi Pengembangan Aplikasi**

   Yang bertujuan untuk menentukan metodologi pengembangan Perangkat Lunak yang digunakan dengan pendekatan terstruktur.

4. **Analisa sistem**

   Melakukan ujicoba dengan menganalisa sistem yang telah dibuat apakah sistem tersebut bekerja dengan baik atau tidak, serta menganalisa kebutuhan yang dibutuhkan dalam pembuatan sistem ini.

5. **Mengambil kesimpulan**

   1. Apakah sistem keamanan RADIUS *server* yang dibuat cukup tangguh untuk diimplementasi oleh ISP pada jaringan mereka.
   2. Apakah pembuatan sistem ini menggunakan sumberdaya yang besar atau sebaliknya.
   3. Apakah sistem ini layak untuk dijadikan sistem keamanan yang bersifat komersial.
   4. Apakah sistem keamanan RADIUS *server* ini dapat mengatasi berbagai macam serangan atau tidak.

5. Jika sistem keamanan RADIUS *server* ini mempunyai kelemahan diharapkan kita dapat menambal lubang dari sistem keamanan ini.

1.6 Sistematika Penulisan

Secara keseluruhan Tugas Akhir ini terdiri dari 5 bab yang secara garis besar penulisan masing-masing bab adalah sebagai berikut :

Bab I PENDAHULUAN

Berisi uraian singkat mengenai latar belakang permasalahan, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, metodologi penelitian, serta sistematika penulisan.

Bab II DASAR TEORI

Bab ini merupakan uraian konsep dan dasar teori yang mendasari penelitian Tugas Akhir yang akan dilakukan.

Bab III PERANCANGAN SISTEM

Bab ini berisi analisa, perancangan dan implementasi dari sistem yang telah dibuat.

Bab IV ANALISIS DAN HASIL PENGUKURAN PARAMETER RADIUS SERVER

Pada bab ini membahas analisis simulasi sistem hasil perancangan dengan pengujian performansi dan parameter keamanan dari RADIUS server.

Bab V PENUTUP

Berisi tentang kesimpulan dan saran terhadap hasil pengujian yang telah dilakukan apakah sudah sesuai dengan standar, serta saran untuk pengembangan sistem keamanan lebih lanjut.

BAB V

PENUTUP

Kesimpulan :

1. Performansi jaringan untuk VPN RADIUS *network* berkurang atau lebih jelek di banding dengan jaringan biasa, dikarenakan adanya proses enkapsulasi data yang menyebabkan ukuran paket data pada VPN RADIUS yang akan dikirim menjadi lebih besar dibandingkan paket yang dikirim pada jaringan biasa.
2. Dari hasil pengukuran *time login* dengan menggunakan *wireshark* untuk panjang *username* 1-8 karakter dihasilkan data sebagai berikut 0.167743, 0.1712, 0.1693495, 0.1775625, 0.167802, 0.173964, 0.173964, 0.22018 (dalam *sekon*). Sedangkan untuk panjang *password* 1-8 karakter dihasilkan data sebagai berikut 0.178409, 0.215473, 0.1773, 0.224204, 0.194394, 0.235199, 0.168114, 0.181997 (dalam *sekon*). Hal ini membuktikan bahwa panjang karakter *username* dan *password* tidak berpengaruh terhadap *time login*. Yang berpengaruh adalah kondisi jaringan kita, jika banyak yang mengakses jaringan maka server akan sibuk dan mengakibatkan kondisi jaringan yang sibuk juga.
3. Dari hasil pengukuran *Delay* dengan menggunakan *wireshark* pada jaringan VPN RADIUS didapatkan rata-rata 1.444737931 *sekon* dan pada jaringan biasa didapatkan *delay* rata-rata sebesar 0.4431552 *sekon*. Hal ini diakibatkan dalam VPN RADIUS *server* terjadi proses enkapsulasi data yang mengakibatkan ukuran paket semakin besar pula sehingga proses pengiriman data menjadi lebih lambat daripada jaringan biasa , hal ini menyebabkan kualitas jaringan turun.
4. Dengan menggunakan software PRTG Traffic Grapher 6.2.1.944 didapatkan data rata-rata *latency* jaringan untuk VPN RADIUS *network* lebih tinggi di banding jaringan biasa, dikarenakan adanya enkapsulasi data yang mengakibatkan proses pengiriman paket menjadi lebih lama dibandingkan jaringan biasa.
5. Untuk keamanannya, saat awal *login*, data yang di kirimkan adalah *username* dan *password*, *username* berupa *plaintext* atau tanpa enkripsi dan *password* di enkripsi dengan algoritma MD5. Hal ini menyebabkan username langsung diketahui dan

saat ini telah ditemukan cara untuk memecah kunci algoritma MD5 yang memungkinkan untuk *cracking password*.

6. Dari hasil pengukuran *throughput* dengan menggunakan *wireshark* didapatkan nilai rata-rata *throughput* pada jaringan VPN RADIUS sebesar 439.5014787 paket/*sekon,* sedangkan pada jaringan biasa didapatkan rata-rata *throughput* sebesar 1487.503881 paket/*sekon.* Throughput pada jaringan VPN RADIUS mempunyai nilai lebih kecil dibandingkan jaringan biasa, hal ini dikarenakan proses enkapsulasi data yang mengakibatkan jumlah paket yang dapat dikirimkan oleh jaringan VPN RADIUS menjadi lebih kecil.

Saran :

1. Untuk lebih lanjut, diharapkan untuk membangun sebuah sistem VPN yang lebih baik, tanpa ada pengurangan performansi jaringan karena proses pada VPN RADIUS terlalu lama memakan waktu.
2. Perlu diteliti lebih lanjut mekanisme pertukaran informasi di dalam RADIUS server itu sendiri, jika memungkinkan sampai tingkat *frame.*
3. Untuk lebih lanjut, perlu di bangun sebuah sistem VPN yang lebih aman, seperti berbasiskan *IPSeC.* Dalam kasus tugas akhir ini digunakan mekanisme CHAP untuk proses dalam RADIUS.
4. Untuk implementasi RADIUS, tidak hanya di ruang lingkup VPN *wired* saja, tetapi ke aplikasi lain seperti VPN *wireless*, VoIP, *video conference*, dll.