RANCANG BANGUN KEAMANAN TRANSFER DATA VOIP *OVER* VPN PADA SISTEM *OPENSOURCE* TRIXBOX

Oleh
I Wayan Eka Putra Darmawan
Jurusan Pendidikan Teknik Informatika

ABSTRAK

VoIP (*Voice over Internet*) dikenal juga dengan sebutan IP (*Internet Protocol*) *Telephony* saat ini semakin banyak digunakan karena memiliki beberapa keunggulan, salah satu diantaranya yaitu tarif yang jauh lebih murah daripada tarif telepon tradisional sehingga pengguna telepon dapat memilih layanan tersebut sesuai dengan kebutuhannya. VoIP dapat mereduksi biaya percakapan sampai 70%. Selain memiliki beberapa keunggulan di atas, VoIP juga memiliki kelemahan yang sangat vital yaitu dari segi keamanan transfer suara karena berbasis IP, sehingga siapapun bisa melakukan penyadapan dan perekaman terhadap data VoIP. Ganguan yang terjadi pada sistem VoIP ada berbagai macam diantaranya, transfer data yang lewat pada suatu jaringan seperti misalnya dapat disalahgunakan *(abuse)*, dapat dibajak isi data tersebut *(sniffing)*, dan tidak dapat mengakses *server* dikarenakan *server* yang kelebihan muatan *(Denial of Services)*.

Ada beberapa cara untuk mengamankan komunikasi data VoIP, antara lain, dengan mengamankan jalur yang digunakan pengguna untuk melakukan komunikasi VoIP dengan menggunakan metode VPN *(Virtual Private Network)* dan juga dapat dilakukan suatu metode kriptografi pada aplikasi VoIP tersebut sehingga data yang dikirimkan dapat dilindungi dengan baik. VPN adalah teknik pengaman jaringan yang bekerja dengan cara membuat suatu *tunnel* sehingga jaringan yang dipercaya dapat menghubungkan jaringan yang ada di luar melalui internet. Titik akhir dari VPN adalah tersambungnya *Virtual Channels* (VCs) dengan cara pemisahan. Kenyataannya koneksi sebuah *end-to-end VPN* tergantung dari sebuah nilai dari hubungan daripada titik-titiknya. VPN mempunyai dua metode dalam pengamanan yakni *IPSec* dan *Crypto IP Encapsulation* (CIPE). Selain itu dapat dipergunakan teknik Kriptografi *(cryptography)* yang merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secara aman.

Sistem VoIP menggunakan VPN ini diharapkan dapat memberikan keamanan transfer data pada jaringan internet maupun intranet.

Kata-kata kunci: *Voice over Internet*, *Virtual Private Network*, *Sniffing*.

ABSTRACT

VoIP (Voice over Internet) also known as IP (Internet Protocol) telephony is increasingly being used because it has several advantages, one of them is far cheaper rates than traditional phone rates so that phone users can choose the service appropriate to their needs. VoIP can reduce costs up to 70% conversation. In addition to having several advantages over, VoIP also has a vital weakness is in terms of security for IP-based voice transfer, so anyone can conduct wiretapping and recording of VoIP data. Disturbance occurs

in the system there are various kinds such as VoIP, data transfer via a network such as for example can be abused (abuse), can be hijacked by the contents of the data (sniffing), and can not access the server because the server is overloaded (Denial of Services).

There are several ways to secure data communications VoIP, among others, to secure the route used by users to make VoIP communications using a VPN (Virtual Private Network) and can also be a method of cryptography in applications such VoIP so that transmitted data can be well protected . VPN is a network of safety technique that works by making a tunnel to a trusted network can connect networks that exist outside the Internet. End point of the VPN is tersambungnya Virtual Channels (VCs) by way of separation. In fact a connection end-to-end VPN hanging from a value from the relationship than the dots. VPN has two methods, namely security and IPSec Crypto IP Encapsulation (CIPE). Moreover, it can be used cryptography techniques (cryptography), which is the science and art of message storage, data, or information securely.

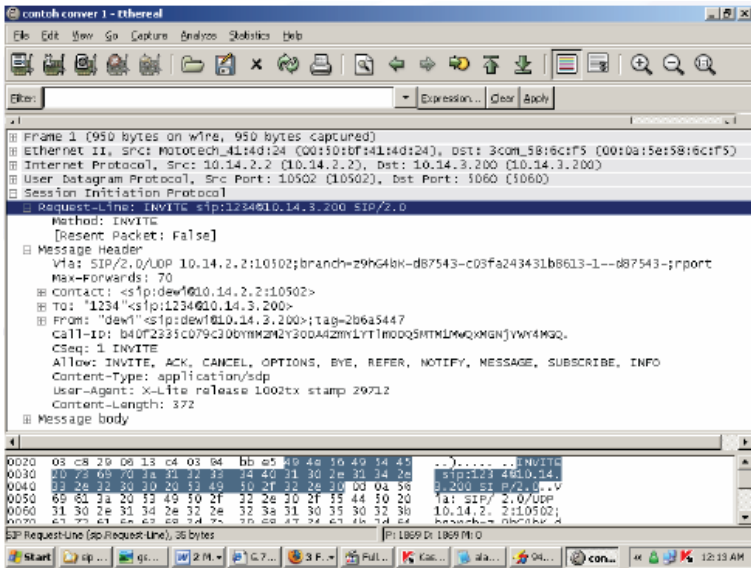
VoIP systems use a VPN is expected to provide security of data transfer on the Internet or intranet network.

Key words: Voice over the Internet, Virtual Private Network, Sniffing.

1. PENDAHULUAN

Voice over Internet Protocol yang disingkat dengan VoIP, dikenal juga dengan sebutan IP (*Internet Protocol*) *Telephony*. VoIP didefinisikan sebagai suatu sistem yang menggunakan jaringan *internet* atau *intranet* untuk mengirimkan data paket suara dari suatu tempat ke tempat yang lain menggunakan perantara protokol IP. Perbedaan VoIP dengan telepon tradisional terletak pada masalah infrastrukturnya. VoIP menggunakan *internet* atau *intranet* sedangakan telepon tradisional menggunakan infrastruktur telepon yang sudah dibangun lebih awal (Winarno, 2008). Teknologi VoIP memiliki beberapa keunggulan, salah satu diantaranya yaitu tarif yang jauh lebih murah daripada tarif telepon tradisional sehingga pengguna telepon dapat memilih layanan tersebut sesuai dengan kebutuhannya. VoIP dapat mereduksi biaya percakapan sampai 70% (Apri, 2009). VoIP telah berhasil memposisikan diri sebagai salah satu kandidat teknologi terbaik pengganti POTS (*Plain Old Telephone Systems*). VoIP terdiri dari dua komponen yaitu *server* dan *client. Server* VoIP berfungsi sebagai basis pemrosesan suara, sedangkan *client* berfungsi sebagai *end* user yang melakukan komunikasi. *VoIP Phone System* berbasiskan sistem *opensource*, dimana yang poluler digunakan adalah Trixbox. Hal ini dikarenakan Trixbox dapat mengkombinasikan paket-paket *opensource* telepon terbaik yang disertakan di dalam sistem operasi tersebut. Selain memiliki beberapa keunggulan di atas, VoIP juga memiliki kelemahan yang sangat vital yaitu dari segi keamanan transfer suara karena berbasis IP, sehingga siapapun bisa melakukan penyadapan dan perekaman terhadap data VoIP. Berikut adalah contoh *sniffing*

yang dilakukan pada jaringan VoIP STT Telkom, *cracker* mengunakan metoda *tapping* dengan menggunakan *software* berbasis windows yaitu cain and abel. Ketika *client* VoIP berkomunikasi, data yang melewati jaringan VoIP disadap dan disalahgunakan oleh *cracker* sehingga sangat menggangu privasi dari pengguna jaringan VoIP STT Telkom. Pada Gambar 1.1 adalah proses penyadapan data yang dilakukan pada jaringan VoIP STT Telkom. (STT Telom, 2007)



Gambar 1 Penyadapan VoIP
(Sumber: STT Telkom, 2007)

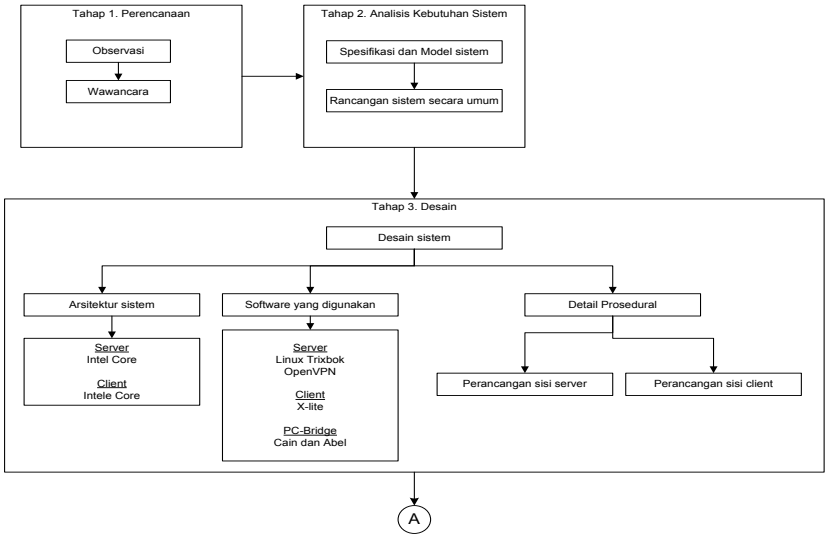
Teknologi VoIP semakin banyak digunakan, tapi teknik keamanan yang digunakan untuk melindungi data hanya beberapa. Adapun macam-macam gangguan *(threats)* data yang lewat pada suatu jaringan seperti misalnya dapat disalahgunakan *(abuse),* dapat dibajak isi data tersebut *(sniffing),* dan tidak dapat mengakses *server* dikarenakan *server* yang kelebihan muatan *(Denial of Services).* Ada beberapa cara untuk mengamankan komunikasi data VoIP, antara lain, dengan mengamankan jalur yang digunakan pengguna untuk melakukan komunikasi VoIP dengan menggunakan metode VPN *(Virtual Private Network)* dan juga dapat dilakukan suatu metode kriptografi pada aplikasi VoIP tersebut sehingga data yang dikirimkan dapat dilindungi dengan baik. VPN adalah teknik pengaman jaringan yang bekerja dengan cara membuat suatu *tunnel* sehingga jaringan yang dipercaya dapat menghubungkan jaringan yang ada di luar melalui internet.

Berdasarkan permasalahan yang telah dijelaskan di atas, maka penulis pada penelitian ini mencoba membuatkan sebuah penelitian dengan judul **"Rancang Bangun**

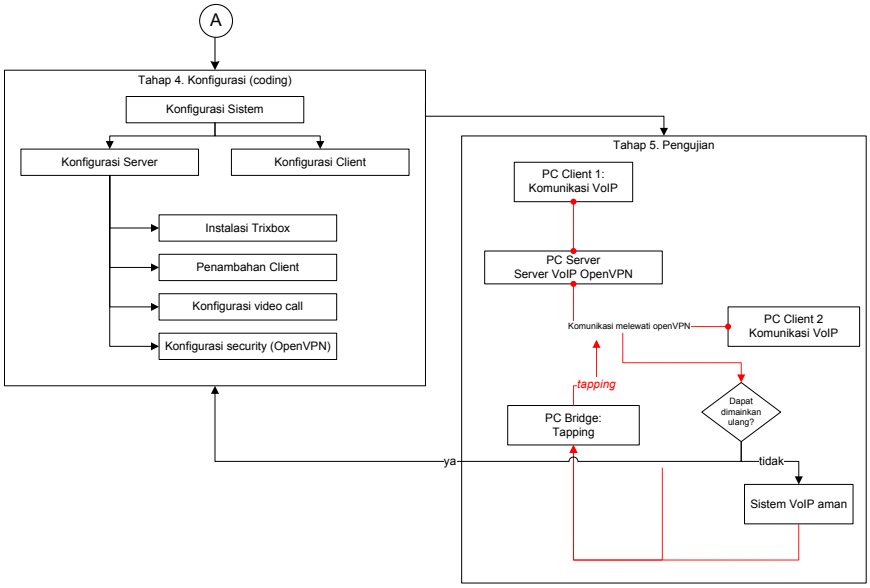
Keamanan Teransfer Data VoIP *over* VPN pada Sistem Opensource Trixbox. Adapun rumusan masalah yang akan dikaji dalam penelitian ini yaitu bagaimana me rancang dan membangun keamanan teransfer data suara VoIP *over* VPN pada sistem *opensource* trixbox?

2. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode *Software Development Life Cycle (*SDLC*)* dengan *Waterfall-based Model.* Pada Gambar 2 dan Gambar 3 dapat dilihat alur pengembangan sistem.



Gambar 2 Bagan pengembangan sistem



Gambar 3 Bagan pengembangan sistem (lanjutan Gambar 2.)

Gambar 2 dan Gambar 3 menunjukan alur dari pengembangan sistem yang dibedakan menjadi beberapa tahap sebagai berikut.

Tahap 1. Perencanaan

Tahap perencanaan dimulai dengan melakukan observasi dan wawancara mengenai permasalahan keamanan transfer data pada saat melakukan komunikasi via VoIP.

Tahap 2. Analisis kebutuhan sistem

Dari permasalahan yang ditemukan pada tahap perencanaan penulis membuat spesifikasi dan model dari kebutuhan pemakai sistem dan membuat alternatif-alternatif rancangan sistem secara umum.

Tahap 3 Desain

Proses desain akan menerjemahkan syarat kebutuhan sistem ke sebuah perancangan sistem yang dapat diperkirakan sebelum konfiguarsi dan *coding* sistem. Proses ini berfokus pada arsitektur sistem, software yang digunakan dan detail prosedural sistem

Tahap 4 Konfigurasi (*coding)*

Pada tahap ini akan dilakukan konfigurasi sistem, dimana merupakan proses realisasi dari desain yang dibuat ke dalam sistem yang dibangun.

Tahap 5 Pengujian

Proses pengujian dilakukan dengan melakukan analisis performansi keamanan serta perubahannya sebelum dan sesudah ditambahkan aplikasi VPN. Untuk membantu analisis keamanan, digunakan alat bantu yaitu *software cain* dan *abel. Software* berbasis *windows* ini akan menangkap semua paket yang lewat dan melakukan analisis keamanan terhadap data VoIP. *Software* ini akan di pasang pada *PC bridge* dan menangkap setiap paket yang melewatinya. Selain itu akan dianalisis isi dari paket tersebut untuk menganalisa celah keamanan lainnya. Skenario yang dibuat adalah VoIP *client* 1 dan 2 akan berkomunikasi dengan menggunakan salah satu *codec*. Kemudian data yang lewat tersebut akan di *tapping* oleh *cain* dan *abel.* Adapun hasil dari *tapping* akan dicoba untuk dimainkan ulang. Apakah rekaman data VoIP tersebut dapat dimainkan ulang, jika ya berarti VoIP menggunakan SIP tidak aman dalam implementasinya dan penulis akan kembali melakukan konfigurasi ulang (kembali ke tahap 4. Konfiguarasi (*coding).* Jika rekaman data tidak dapat dimainkan ulang maka sistem VoIP *over* VPN sudah aman.

Instrumen yang digunakan untuk analisis sistem adalah berupa angket, untuk lebih jelasnya dapat dilihat pada tabel 1, tabel 2, tabel 3, dan tabel 4

Tabel 1. Pengujian koneksi

No	Mekanisme pengujian	Indikator pengujian	Hasil Pengujian	
			Ya	Tidak
1	Komputer *server* maupun komputer *client* menjalankan perintah "ping 127.0.0.1"	Ketika menjalankan perintah ping apakah muncul tampilan seperti gambar 3.3		

Tabel 2. Pengujian *server*

No	Mekanisme pengujian	Indikator pengujian	Hasil Pengujian	
			Ya	Tidak
1	Komputer *server booting* dengan normal sampai proses berakhir ditandai dengan muculnya halaman *login* pada layar monitor	Layar monitor muncul tampilan awal *login user*		
2	Komputer *server* dapat dikonfigurasi melalui *remote web base* sampai ke tahap halaman *login user*	User bisa membuka halaman *login user* melalui halaman web		
3	Komputer *server* dapat menambahkan serta ter-*register extension* dari VoIP *client* ketika dikonfigurasi melalui *remote web base*	Administrator dapat menambahkan VoIP *extension*		
4	Komputer *server* dapat menjalankan OpenVPN *Server*	OpenVPN dapat dijalankan dengan baik		

Tabel 3. Pengujian *client*

No	Mekanisme pengujian	Indikator pengujian	Hasil Pengujian	
			Ya	Tidak
1	VoIP *client* atau s*oftphone x-lite* sudah terinstal dengan benar	PC *client* sudah terinstal X-Lite		

2	di PC *client* VoIP *client* sudah teregister dengan baik dan siap melakukan panggilan	VoIP *client* bisa terhubung ke s*erver* VoIP		

Tabel 4. Pengujian Kemanan VoIP *over* VPN

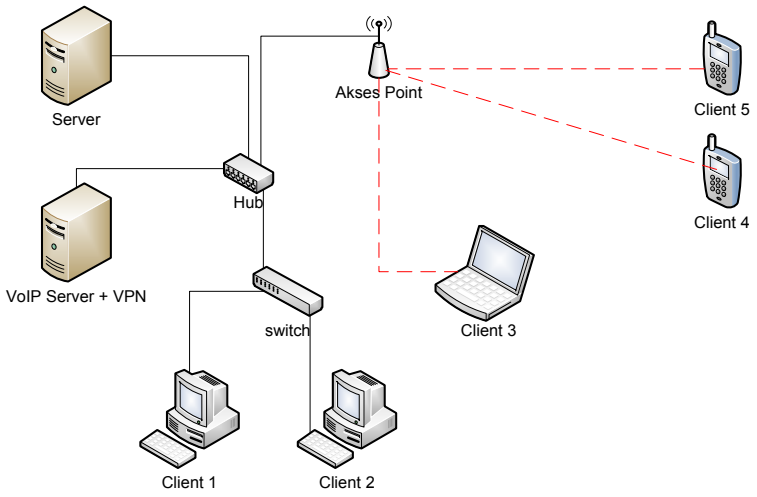
No	Mekanisme pengujian	Indikator pengujian	Hasil Pengujian	
			Ya	Tidak
1	PC client 1 berkomikasi dengan PC client 2 menggunakan openVPN dan PC brige melakukan sniffing dengan *software* cain dan abel	Transfer data antara pc client 1 dan 2 dapat di tangkap oleh pc brige dan dimainkan ulang		

3. HASIL DAN PEMBAHASAN

Dalam pembuatan sistem jaringan IP *telephony* atau VoIP akan dilakukan prosedur operasi dan pengujian yang mengacu pada desain perancangan . Ada beberapa tahap yang harus dilakukan yaitu sebagai berikut:

1. Konfigurasi pada sisi *server*
   a. Instalasi Trixbox
   b. Penambahan *Client*
   c. Konfigurasi *Video Call*
   d. Konfigurasi *Security*
2. Konfigurasi pada sisi *client*
3. Pengujian pada sisi *server*
4. Pengujian pada sisi *client*
5. Pengujian sistem

Implementasi dan prosedur operasi pada jaringan IP *telephony* atau VoIP sistem akan dilakukan sesuai dengan langkah-langkah di atas. Pada pengujian sistem akan dilakukan beberapa pengujian agar sistem bisa diketahui dapat berjalan dengan normal serta dapat dianalisa keamanan dalam IP *telephony* tersebut. Pada gambar 4bisa dilihat pemetaan dari jaringan yang akan dibuat.



Gambar 4 Pemetaan Jaringan VoIP.

Spesifikasi dari kebutuhan *hardware* dan *software* komputer *server* dan komputer *client* bisa dilihat pada Tabel 5

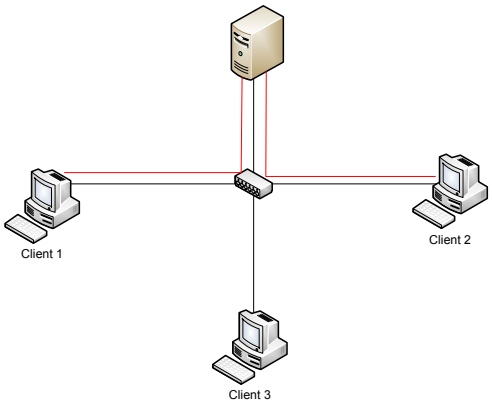
Tabel 5 Dafar Perangkat

No	Jenis Perangkat	Interface	IP	Sistem Operasi	Aplikasi yang digunakan
1	VoIP Server	Eth0	11.11.1.4	Linux Trixbox	Asterisk OpenVPN
2	Dua komputer VoIP client	Eth0	11.11.1.100 11.11.1.101	Microsoft Windows Seven	*Softphone* X-LIte
3	Dua *Handphone* ber-wifi	Mobile Wifi	11.11.1.102 11.11.1.103	Symbian 9 versi 3	SIP *Connection*
4	PC *bridge*	Eth0	11.11.1.104	Microsoft Windows *Seven*	Cian dan Abel

Pengujian keamanan dengan cara penyadapan terhadap panggilan VoIP yang sedang berjalan dalam jaringan lokal. Langkah-langkahnya adalah sebagai berikut :

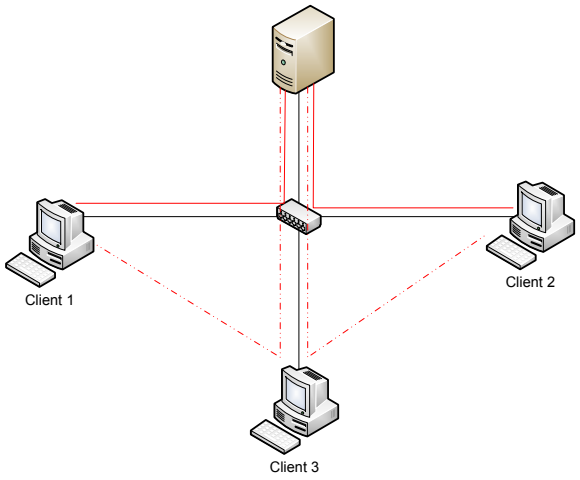
a. PC yang berfungsi sebagai penyadap ditambahkan program *Cain & Able* yang diambil dari http://www.oxid.it/. Langkah-langkah instalasi secara detail dapat dilihat pada lampiran.

b. Ketika panggilan sedang berlangsung dari *client 1* menuju *client 2* alur data pada jaringan ditunjukkan dengan garis merah pada Gambar 5. Komputer pada *client1* akan mengirimkan data menuju *server* untuk dilanjutkan dari *server* menuju *client2*.



Gambar 5 Alur Data Panggilan

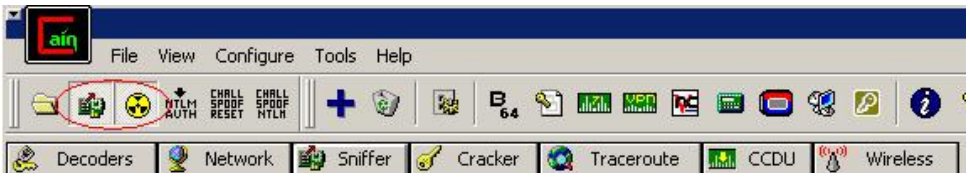
c. Ketika data akan disadap komunikasi antara *client 1* menuju *server* akan dialihkan terlebih dahulu menuju *client 3 (sniffer)* dan baru akan diteruskan menuju *server*. Begitu juga proses antara *client 2* menuju *server* akan dialihkan terlebih dahulu menuju *client 3 (sniffer)*. Sehingga data percakapan *client 1* dan *client 2* akan disadap oleh *client 3* seperti pada Gambar 6



Gambar 6 Penyadapan Data

Cara penyadapan yang dilakukan *client 3* adalah dengan langkah-langkah sebagai berikut :

a. Pembukaan program *cain abel* pada *Start Menu > All Program > Cain*
b. Aktifkan proses *sniffing* dan *ARP poison routing* dengan menekan *start sniffer* dan *start poison routing* seperti pada Gambar 7..

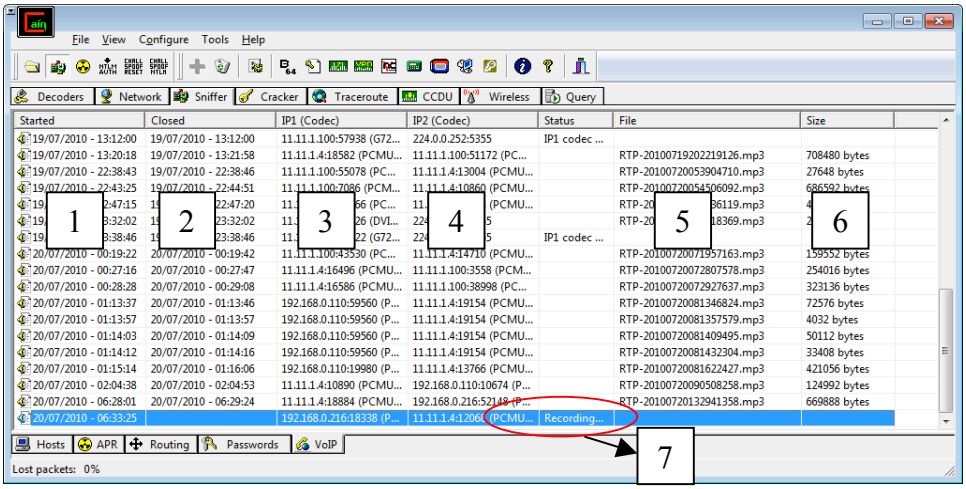


Gambar 7 Menjalankan *Sniffing* dan *Poison Routing*

c. Pada program *Cain* buka *tab Sniffer* > *Host* kemudian pilih *add host* pada *tool bar*. Maka akan muncul *dialog box* untuk me-*scan* IP komputer *VoIP client* yang lain dalam jaringan.

d. Pada *tab sniffer* pilih sub *tab ARP*. Tambahkan *host* yaitu *host* dari sisi *server* dan *client* yang akan disadap kemudian pilih *tab sniffer* > *VoIP* untuk melihat komunikasi VoIP yang sedang berjalan.

e. Contoh penyadapan yang dilakukan pada *server* VoIP dapat dilihat pada gambar 8.



Gambar 8. Penyadapan VoIP

Gambar 8 adalah proses penyadapan komunikasi VoIP dengan *software* Cain dan Abel. Berikut adalah penjelasan angka yang tertera pada gambar.

a) Nomor 1, menunjukan tanggal dan waktu dimulainya komunikasi melalui jaringan VoIP.

b) Nomor 2, menunjukan tanggal dan waktu berakhirnya percakapan yang dilakukan melalui jaringan VoIP.

c) Nomor 3, menunjukan alamat IP dari VoIP *client* 1 yang melakukan panggilan ke VoIP *client* 2.

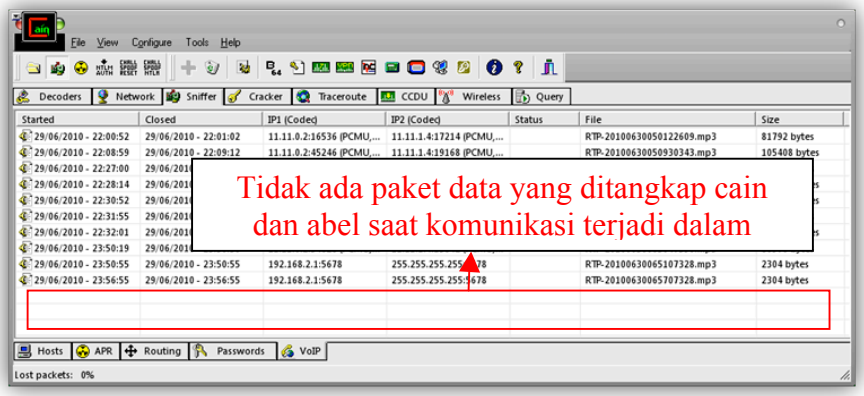
d) Nomor 4, menunjukan alamt IP dari VoIP *client* 2 yang merupakan penerima telepon dari VoIP *client* 1.

e) Nomor 5, adalah jenis *codec* yang dihasilkan dari penyadapan komunikasi antara *client* 1 dan *client* 2, yang bisa dimainkan ulang oleh penyadap.

f) Nomor 6, menunjukan ukuran *file codac* yang tersimpan di komputer penyadap.

g) Nomor 7, adalah proses penyadapan ditandai dengan tanda *recording* saat proses percakapan terjadi antara *client* 1 dan *client* 2.

Pengujian keamanan dilakukan kembali dengan melakukan *sniffing* untuk membuktikan bahwa jaringan menggunakan VPN bersifat lebih aman. Gambar 9. menunjukan *software* cain dan abel tidak dapat menangkap alur komunikasi yang terjadi pada sistem VoIP.



Gambar 9. Tampilan cain dan abel yang tidak bisa menangkap transfer data yang berlangsung dijaringan VoIP

4. PENUTUP

Berdasarkan hasil analisis data dan pembahasan pada penelitian ini, maka dapat diambil simpulan yaitu : (1)Secara garis besar sistem operasi *trixbox* sudah dapat digunakan untuk menangani jaringan IP *telephony*, namun ketika dilakukan penyadapan dengan menggunakan program *cain able* terbukti komunikasi suara dapat terekam sehingga privasi dari pengguna VoIP kurang terjamin.Untuk mengatasi penyadapan, maka diberi salah satu alternatif pengamanan dengan melakukan penambahan VPN *server* pada *trixbox*, serta penambahan VPN *client* pada sisi client VoIP sehingga trafik VoIP dilewatkan melalui koneksi VPN.(2) Penggunaan VPN menjadikan sistem VoIP aman dikarenakan adanya autentikasi antara *server* dan *client* ketika akan melakukan koneksi, serta pemberian enkripsi

pada data yang akan dikirim.(3) Penggunaan VPN tidak mempengaruhi kemampuan komunikasi VoIP dalam jaringan lokal.

Berdasarkan pengamatan penulis, terdapat beberapa hal yang dapat dijadikan bahan pertimbangan untuk ditindak lanjuti diantaranya: (1) Penggunaan VoIP merupakan solusi alternatif komunikasi masa depan, oleh karena itu untuk pengembangan selanjutnya dapat dilakukan analisis performansi VoIP dengan VoIP monitoring. (2) Disarankan untuk penggunaan VPN dalam jaringan internet agar lebih memperhatikan *delay* dari transfer suara VoIP. (3) Bagi pengguna yang ingin menghubungkan VoIP dengan telepon konvensional disarankan untuk menambahkan modul telepon *gateway*.

DAFTAR PUSTAKA

Farhan Perdana, 2007. ”Sniffing? Cain & Abel Saja!”. Tersedia pada http://ilmukomputer.org/2007/03/27/sniffing-cain-abel-saja/ (diakses tanggal 10 Maret 2010).

Rossadhi S. Sany, 2009. ”Teknik Keamanan Voice over WLANs 802.11”. Universitas Sumatra Utara.

Sugeng Winarno, 2008. ”Membangun Telepon Berbasis VoIP”. Bandung: Informatika.