

**ANALISIS DAN PERANCANGAN SECURITY VOICE OVER INTERNET  
PROTOKOL ( VoIP ) MENGGUNAKAN GNU LINUX TRIBOX PADA  
JARINGAN LOKAL**

**Naskah Publikasi**



diajukan oleh

**Andri Yansyah Putra**

**09.21.0461**

**Kepada**

**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**

**AMIKOM**

**YOGYAKARTA**

**2010**

**NASKAH PUBLIKASI**

**ANALISIS DAN PERANCANGAN SECURITY VOICE OVER INTERNET  
PROTOKOL ( VoIP ) MENGGUNAKAN GNU LINUX TRIBOX PADA  
JARINGAN LOKAL**

Disusun oleh

**Andri Yansyah Putra**

**09.21.0461**

**Dosen Pembimbing**

**Melwin Syarifal, S.Kom., M.Eng.**  
**NIK. 190302105**

**Tanggal 11 November 2010**

**Ketua Jurusan  
Teknik Informatika**

**Ir. Abas Ali Pangera, M. Kom.**  
**NIK. 190302010**

**SYSTEM SECURITY ANALYSIS AND DESIGN VOICE OVER  
INTERNET (VOIP ) GNU LINUX USING TRIXBOX ON LOCAL  
NETWORK**

**ANALISIS DAN PERANCANGAN SECURITY VOICE OVER INTERNET  
PROTOKOL ( VoIP ) MENGGUNAKAN GNU LINUX TRIBOX PADA  
JARINGAN LOKAL**

Andri Yansyah Putra

Jurusan Teknik Informatika

STMIK AMIKOM YOGYAKARTA

**ABSTRACT**

*Spur the development of technology today to make the technology more affordable or unaffordable. Network grows increasingly fast computers that allow voice traffic to pass through a common computer network or called VoIP (Voice Over InternetProtocol).*

*The use of VoIP technology is considered as one of the cheaper alternative with the ability to provide such service line extension, Video Call, VoIP calls to PSTN, PSTN to VoIP calls, and digital receptionist (IVR). But the weakness of the security system here is VoIP VoIP calls that can be done tapping.*

*To overcome this weakness, VoIP communication is done by using a VPN is fast, easy and cheap. Process Analysis and design of security in VoIP systems consists of configuration and testing. Security testing was assessed with voice communication can not be tapped, which means privacy of VoIP users is guaranteed.*

**Keyword :** VoIP, Video Call, VPN, VoIPTo PSTN, PSTN to VoIP, IVR

## BAB I

### PENDAHULUAN

#### 1.1 Latar Belakang Masalah

Seiring pesatnya perkembangan jumlah komputer yang saling terhubung dengan lainnya dan yang biasa disebut dengan jaringan komputer. Teknologi yang saling menghubungkan komputer di dunia memungkinkan untuk dapat saling bertukar informasi dan data, bahkan dapat saling berkomunikasi dan bertukar informasi berupa gambar atau video . Perkembangan jaringan komputer yang semakin pesat memungkinkan untuk melewati trafik suara melalui jaringan komputer atau biasa yang disebut VoIP (Voice Over Internet Protocol).

VoIP adalah teknologi yang menawarkan telepon melalui jaringan IP (*Internet Protocol*) dengan teknologi ini mengubah suara menjadi kode digital melalui jaringan paket-paket data, bukan sirkuit analog telepon biasa. Penggunaan jaringan IP memungkinkan penekanan biaya dikarenakan tidak perlu membangun sebuah infrastruktur baru untuk komunikasi suara dan penggunaan lebar data (*bandwidth*) yang lebih kecil dibandingkan telepon biasa.

Penggunaan teknologi VoIP yang lebih efisien akan semakin dipermudah karena dapat digabungkan dengan jaringan telepon lokal yang sudah ada, dengan menggunakan VoIP *gateway* yang akan disambungkan dengan PABX. Setiap individu dapat membangun dan mengembangkan. Infrastrukturnya secara mandiri, dikarenakan penggunaan sistem operasi berbasis linux / *open source* Trixbox yang memang dikhususkan untuk menangani VoIP.

Penggunaan teknologi VoIP jelas menguntungkan bagi penggunanya. Namun, penggunaan komunikasi yang murah dari sisi keamanan kurang begitu di perhatikan. Oleh karena itu keamanan ketika melakukan komunikasi suara merupakan sesuatu yang sangat penting , karena menyangkut privasi penggunanya. Penggunaan VPN (Virtual Private Network) merupakan salah satu alternatif pelewatan komunikasi suara , yang bersifat private atau aman , karena penggunaan koneksi yang telah terenkripsi serta penggunaan private keys, certificate, atau username/password untuk melakukan autentikasi dalam membangun koneksi.

## **1.2 Rumusan Masalah**

Berdasarkan latar belakang di atas, maka rumusan masalah yang dapat diambil adalah bagaimana Menganalisis serta membangun jaringan telpon berbasis IP menggunakan VPN sebagai keamanan komunikasi VoIP dalam jaringan Lokal

## **1.3 Batasan Masalah**

Ruang lingkup dalam penyusunan skripsi ini adalah, terbatas pada pengaturan dan konfigurasi VoIP server Trixbox, penggunaan VoIP gateway untuk melakukan panggilan dari VoIP client ke nomor Client yang lain, dan pemanggilan *Video Call* antar client beserta penggunaan OpenVPN sebagai implementasi keamanan dalam jaringan VoIP. Serta penjadapan komunikasi VoIP Trixbox.

## **BAB II**

### **LANDASAN TEORI**

#### **2.1 Tinjauan Pustaka**

Penelitian Sanny Rossadhi ( 041401063 ) Departemen Ilmu Komputer, Fakultas Matematika Dan Ilmu Pengetahuan Alam, Universitas Sumatera Utara 2009, yang berjudul “ Teknik Keamanan Voice Over Wlans 802.11 ”, membahas VPN sebagai pengamanan jaringan yang bekerja dengan cara membuat suatu tunnel sehingga jaringan yang dipercaya dapat menghubungkan jaringan yang ada di luar melalui internet. Dalam Penulis akan mencoba melakukan penelitian dan simulasi tentang keamanan jaringan voip dengan menggunakan konsep *Virtual Private Network ( VPN )* pada jaringan lokal menggunakan linux trixbox

Penelitian Rizal Ansyori ( G64103051 ) Departemen Ilmu Komputer, Fakultas Matematika Dan Ilmu Pengetahuan Alam, Institut Pertanian Bogor 2008, yang berjudul “ Desain, Implementasi, Dan Analisis Interkoneksi Antara Protokol H.323 Dan Sip Pada Jaringan Voip “ , yang menghubungkan protokol H.323 dengan SIP pada jaringanVoIP. Dan Media perantara interkoneksi protokol H.323 dan SIP menggunakan suatu aplikasi *open source* berbasis Linux yang bernama Asterisk yang dikenal sebagai salah satu *signaling gateway*.

Dari para peneliti di atas semua membahas tentang teknologi voice , serta membahas keamanan jaringan VPN. Maka penulis akan membuktikan dan mengimplementasikan teknologi tersebut. Perbedaan penelitian ini sama peneliti di atas yaitu penulis langsung mengimplementasikan jaringan voip dengan menggunakan asterisk pada sistem operasi linux TrixboxCE yang sudah terpaket didalamnya. Serta mengimplementasikan Jaringan Virtual Private Network (VPN) sebagai metode keamanan pada jaringan voip linux TrixboxCE.

#### **2.2 Jaringan Komputer**

Jaringan komputer adalah kumpulan dua komputer atau lebih yang secara cerdas yang saling berbagi-pakai alat-alat hardware dan software . Jaringan bisa terbentuk dari minimal dua komputer sederhana dan kecil yang saling berbagi-pakai printer dan CD-ROM yang terpasang pada salah satu komputer. Namun jaringan bisa berbentuk jalinan saluran komputer terbesar di dunia yaitu internet.

### 2.3 VOIP

VoIP (*Voice Over Internet Protocol*) adalah teknologi berupa *hardware* atau *software* yang memungkinkan percakapan telepon dengan menggunakan jalur komunikasi data pada suatu jaringan komputer. Teknologi ini dengan cara merubah suara menjadi format digital tertentu sehingga dapat dilewatkan melalui jaringan IP.

### 2.4 Keamanan Jaringan

Keamanan jaringan komputer adalah proses untuk menghindari atau melindungi dari gangguan baik untuk pencurian data, manipulasi data. Penggunaan sistem keamanan yang baik maka akan menjadikan komunikasi data pada komputer akan semakin aman.

### 2.5 Mekanisme Keamanan VoIP

Solusi keamanan untuk VoIP bisa dibagi menjadi dua kelompok dasar, singnaling (SIP) dan media (RTP) berhubungan dan menganggap beberapa isu dasar *encryption*, *authentication* dan *key distribution* :

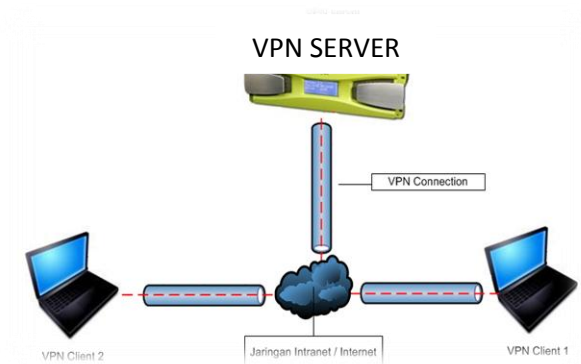
### 2.6 Trixbox CE

*Trixbox CE ( Community Edition)* adalah sebuah *VoIP Phone System* berbasiskan sistem *open source* paling populer didunia karena mengkombinasikan paket-paket *Open Source* telepon terbaik yang disertakan didalam sistem operasi tersebut. Sebelumnya kebanyakan *user* yang ingin mengimplementasikan teknologi VoIP harus dengan usaha yang besar dikarenakan harus menjadi seorang *programer* untuk menghadapi *user interface* yang tidak *friendly* , oleh karena itu untuk mengatasi masalah seperti itu diluncurkannya *trixbox* dengan penggunaan yang sangat mudah karena menu utama yang berbasiskan *web* untuk menkonfigurasi dan mengatur sistem,serta paket-paket untuk VoIP Server dijadikan dalam satu *bundle* dengan *operating system CentOS* sehingga menjadi sistem *TrixboxCE*.

### 2.7 Virtual Private Network (VPN)

VPN (*Virtual Private Network*) adalah teknik pengamanan jaringan dengan cara membuat suatu *tunnel* misalkan pada jaringan publik atau internet sehingga jaringan bersifat *private* dan aman. VPN dikatakan bersifat *private* karena ketika akan terbentuknya sebuah koneksi VPN dibutuhkan *authentikasi* untuk memastikan bahwa kedua ujung dalam koneksi adalah *user* yang sesuai yang diberi kewenangan untuk mengakses suatu *server*. Setelah terbentuknya suatu koneksi VPN maka data akan di *enkripsi* untuk menjaga kerahasiaan paket yang dikirimkan. Penggunaan autentikasi

dan enkripsi yang dipadukan dalam VPN membuat suatu system keamanan yang lebih baik seperti pada Gambar 2.9.



**Gambar 2.9** Pelewatan data dengan VPN

## 2.9 OpenVPN

*OpenVPN* adalah salah satu aplikasi VPN berbasis *open source* untuk membuat koneksi *encrypted tunnels* secara virtual dengan menggunakan authenticate dengan yang lainnya menggunakan pre-shared secret key, certificates, atau username. *OpenVPN* memiliki beberapa kelebihan untuk membuat VPN server seperti berbasis *open source*, keamanan, kesetabilan, mekanisme autentikasi dan enkripsi.



## **BAB III**

### **ANALISIS DAN PERANCANGAN SISTEM**

#### **3.1 Tinjauan Kasus**

Perkembangan teknologi Voice over Internet Protocol (VoIP) sejak dikembangkan pada tahun 1995 sudah semakin pesat. Awalnya dianggap “nyeleneh” tapi sekarang menjadi harapan pengguna sebagai alternatif telepon murah. Namun di Indonesia masih ribut pada masalah regulasinya. Mulai dari substansinya sampai siapa yang berwenang membuat regulasinya. “Ketakutan” akan penurunan pendapatan oleh operator telokomunikasi juga mempengaruhi regulasi pemerintah.

VoIP sebenarnya adalah aplikasi internet biasa seperti layanan www dan email. VoIP sebagai layanan Internet biasa disebut IP Telephony. VoIP dapat berjalan di jaringan LAN maupun pada jaringan WAN, Infrastruktur internet dibutuhkan agar dapat menggunakan dan atau menyediakan layanan VoIP. Secara umum, VoIP didefinisikan sebagai suatu sistem yang menggunakan jaringan Lokal maupun jaringan internet untuk mengirimkan data paket suara dari suatu tempat ke tempat yang lain menggunakan perantara protokol IP.

Pada suatu kantor atau pada jaringan lokal, biasanya sudah terdapat layanan Private Branch eXchange (PBX) lokal, yang memudahkan antar divisi untuk menelpon ke divisi yang lainnya. Pegawai yang ingin menghubungi ke pegawai yang lainnya tinggal menekan nomor extension yang ingin dihubungi, tanpa perlu terkoneksi melalui PSTN. Makin kedepan, teknologi berjalan semakin canggih, perkembangan software open source juga turut ambil alih dalam mengembangkan beragam layanan PBX. Dunia free dan open source software juga turut menyumbang besar dengan merilis paket aplikasi IP PBX bernama asterisk. Dengan menggunakan software Asterisk, kini suatu kantor dapat membuat layanan PBX berbasis IP. Dengan menggunakan Asterisk TrixboxCE, layanan IP PBX ini juga dapat semakin diperluas sehingga kantor yang memiliki banyak divisi akan mudah berkomunikasi dengan divisi yang lainnya, Hal ini tentunya dapat menghemat biaya komunikasi antar divisi, yang biasanya dihitung sebagai SLJJ atau SLI jika melakukan komunikasi via telpon biasa.

Akan tetapi, dari proses komunikasi jaringan lokal yang berjalan, dapat memunculkan penyadapan suara dari komunikasi yang sedang berlangsung, dan hal ini tentunya dapat merugikan bagi setiap divisi, karena pentingnya informasi bagi divisi, ternyata masih bisa di sadap dari pihak yang tidak diberikan izin untuk mengetahui informasi yang sedang berlangsung.

Setelah melihat dari kenyataan tersebut maka sangat diperlukannya sistem keamanan jaringan VoIP, untuk menghindari pencurian atau penyadapan dari pihak yang tidak bertanggung jawab. Oleh karena itu penulis akan membangun serta mengimplementasikan keamanan jaringan pada jaringan VoIP, guna menjaga kestabilan jaringan VoIP yang akan di bangun. Beberapa hal yang akan di bahas antara lain,

1. Perancangan Diagram Jaringan Menentukan besarnya jaringan yang di akan bangun
2. Perancangan Server, Membangun server VoIP menggunakan linux Trixbox
3. Perancangan Vpn Server, Menentukan Server VPN sebagai sentral keamanan VoIP
4. Perancangan Voip Client, Menentukan Client VoIP sekaligus sebagai VPN Client

### **3.2 Analisis Sistem**

Analisis dan perancangan keamanan jaringan VoIP menggunakan Linux TrixboxCE adalah sebagai langkah awal untuk membangun konsep rancangan system yang akan di bangun, untuk menghasilkan output yang optimal. Keamanan jaringan VoIP merupakan system yang dibangun untuk menghindari pengaksesan dari client yang tidak di iijinkan.

### **3.3 Pengertian Analisis Sistem**

Analisis sistem dapat didefinisikan sebagai penguraian dari suatu komponen informasi yang utuh kedalam bagian-bagian komponennya, dengan maksud untuk mengidentifikasikan dan mengevaluasi permasalahan-permasalahan, kesimpulan-kesimpulan, hambatan-hambatan yang terjadi, serta kebutuhan-kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan-perbaikannya

### **3.4 Identifikasi Masalah**

Tinjauan kasus yang telah di identifikasi oleh penulis adalah sebagai berikut :

1. Penggunaan layanan VoIP memerlukan suatu perangkat khusus, seperti server dan client. Kedua perangkat tersebut menggunakan protocol H323.  
Penggunaan perangkat ini mudah digunakan karena pengalamatan nya menggunakan IP *Unicast*. Sehingga dapat melakukan tranmisi informasi *Point To Point* Atau *Peer To Peer*.
2. Pelaksanaan uji coba yang dilakukan menemukan kendala-kendala, antarlain PC hanya tersedia 4 perangkat. Sehingga memerlukan kabel UTP yang cukup

panjang dan Hub / Switch untuk menghubungkan antara PC satu dengan yang lainnya.

3. Aplikasi softphone yang ada tidak dapat mengirim gambar dan font yang berbeda
4. Belum ada server khusus untuk layanan komunikasi, sehingga dapat mengganggu komunikasi data.

### 3.5 Analisis Kebutuhan Perangkat Keras (Hardware)

Bagian ini menjelaskan hardware yang digunakan dalam proses perancangan keamanan jaringan *VoIP Linux TrixboxCE* dan digunakan pada saat system berjalan. Dalam menyelesaikan penelitian ini, penulis menggunakan beberapa komputer PC dan laptop, yang berperan sebagai *Server* dan *Client*. Adapun spesifikasi perangkat keras yang digunakan sebagai berikut :

1. Komputer PC yang berfungsi sebagai *Server Trixbox* Sekaligus *VPN Server*
  - a) Motherboard : Intel Cooperation
  - b) Prosesor : Intel Pentium(R)CPU E5300 @ 2.60GHz (2CPUs)
  - c) VGA : Intel (R) 82945G Express Chipset Family
  - d) Memory : NVidia 1024 MB RAM
  - e) Hardisk : 10 GB
  - f) Lan Card : Realtek RTL8139/810x Family Fast Ethernet NIC
2. Laptop yang berfungsi Client *VoIP* sekaligus *VPN Client*3 perangkat.
  - a) Motherboard : Intel Cooperation
  - b) Prosesor : Intel Pentium(R)CPU E5300 @ 2.60GHz (2CPUs)
  - c) VGA : Intel (R) 82945G Express Chipset Family
  - d) Memory : NVidia 1024 MB RAM
  - e) Hardisk :160 GB
  - f) Lan Card : Realtek RTL8139/810x Family Fast Ethernet NIC
3. Kabel : UTP
4. Konektor : RJ45 untuk disambungkan ke kabel RJ45
5. Hub / switch : Sebagai alat untuk menghubungkan jaringan lokal

### 3.6 Analisis Kebutuhan Perangkat Lunak (Software)

Perangkat lunak juga merupakan perangkat yang sangat penting dalam proses pembuatan system, karena perangkat lunak berisikan program yang perintahnya digunakan untuk menjalankan system komputer. Adapun software yang digunakan dalam proses pembangunan keamanan jaringan *VoIP TrixboxCE*

- a) System operasi *Linux TrixboxCE 2.8.03*

Merupakan Platform Sistem Operasi yang digunakan dalam pembuatan system VoIP

**b) Sistem operasi *Windows***

Saat ini sistem operasi *Windows* sudah dikembangkan, tetapi ada software yang dijalankan tidak selancar linux dan sistem keamanan di windows tidak sebaik di linux. Sistem operasi ini akan digunakan untuk kebutuhan *Client* yang sifatnya *User Friendly*

**c) OpenVPN**

Merupakan *VPN Server* untuk membuat jaringan pribadi antara *VPN Server* Dan *VPN Client*

**d) X-Lite**

Sebagai Softphone pada komputer client

**e) Putty**

Software untuk meremot server linux trixboxCE

**f) Cain & Able**

Sebagai Software untuk pengujian keamanan VPN

### **3.7 Analisis Kelayakan Sistem**

Studi kelayakan adalah studi yang akan digunakan untuk menentukan kemungkinan apakah pengembangan proyek system layak di teruskan atau dihentikan. Studi kelayakan merupakan kepadatan versi ringkasan dari keseluruhan analisis sistem dan proses pembuatan sistem keamanan jaringan VoIP Linux TrixboxCE 2.8.03. Fase ini merupakan fase yang penting dan akan dilakukan studi kelayakan terhadap sistem yang akan dibuat.

Studi kelayakan akan menilai dari berbagai sisi, apakah system layak atau tidak. Analisis kelayakan merupakan tahap yang paling penting, karena didalamnya menyangkut berbagai aspek system baru yang di usulkan.

## BAB IV

### IMPLEMENTASI DAN PEMBAHASAN

#### 4.1 Konfigurasi Security

Konfigurasi *security* atau keamanan dalam VoIP dalam hal ini menggunakan *OpenVPN* sebagai pelewatan data VoIP. Langkah-langkah instalasi *OpenVPN* versi 2.09 seperti berikut :

1. Download instalasi file *openVPN* serta file dependensinya untuk sistem operasi CentOS pada <http://dag.wieers.com/rpm/packages/openvpn/> untuk file *openvpn-2.0.9-1.el5.rf.i386.rpm* serta <http://dag.wieers.com/rpm/packages/lzo2/> untuk file *lzo2-2.02-3.el5.rf.i386.rpm*.
2. Salin File yang telah di download ke dalam *Trixbox* dengan menggunakan media *flashdisk* atau menggunakan protokol *SCP (Secure Copy)*.
3. Buka *konsole* pada *server*
4. Lakukan *mount* pada *flashdisk* dengan perintah *mount -a* kemudian pindah ke *directory /etc/media/* salin file *openvpn-2.0.9-1.el5.rf.i386.rpm* serta *lzo2-2.02-3.el5.rf.i386.rpm* kedalam */root/*
5. Pindah kedalam *directory /root/* dengan perintah *cd /root*
6. ketik perintah *ls* untuk menampilkan isi *directory root* seperti Gambar 4.14

```
[trixbox1.localdomain ~]# ls
anaconda-ks.cfg  install.log.syslog  lzo2-2.02-3.el5.rf.i386.rpm
install.log      install_trixbox.log openvpn-2.0.9-1.el5.rf.i386.rpm
[trixbox1.localdomain ~]#
```

Gambar 4.5 Melihat Isi Directory Root

7. Install *dependensi* yang dibutuhkan *openVPN* dengan perintah *rpm -ivh -2.02-3.el5.rf.i386.rpm* sehingga proses instalasi akan berjalan seperti pada Gambar 4.15

```
[trixbox1.localdomain ~]# rpm -ivh lzo2-2.02-3.el5.rf.i386.rpm
warning: lzo2-2.02-3.el5.rf.i386.rpm: Header V3 DSA signature: NOKEY, key ID 6b8d19e6
Preparing... ##### [100%]
 1:lzo2 ##### [100%]
[trixbox1.localdomain ~]#
```

Gambar 4.6 Instalasi dependensi yang dibutuhkan openVPN

8. Install *OpenVPN* dengan perintah `rpm -ivh openvpn-2.0.9-1.el5.rf.i386.rpm` sehingga proses instalasi akan berjalan seperti pada Gambar 4.16

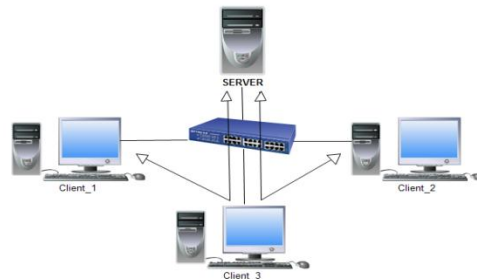
```
[trixbox1.localdomain ~]# rpm -ivh openvpn-2.0.9-1.el5.rf.i386.rpm
warning: openvpn-2.0.9-1.el5.rf.i386.rpm: Header V3 DSA signature: NOKEY, key ID
6b8d79e6
Preparing... ##### [100%]
 1:openvpn ##### [100%]
```

**Gambar 4.7** Instalasi Openvpn

Setelah proses instalasi *OpenVPN* selesai maka akan dilakukan pembuatan *Certificate Authority (CA)* dan *keys* untuk autentikasi

## 4.2 Pengujian Penyadapan

Ketika data akan disadap komunikasi antara client 1 menuju server akan di alihkan terlebih dahulu menuju *client 3 (sniffer)* dan baru akan di teruskan 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 4.25



**Gambar 4.25** Penyadapan Data.

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

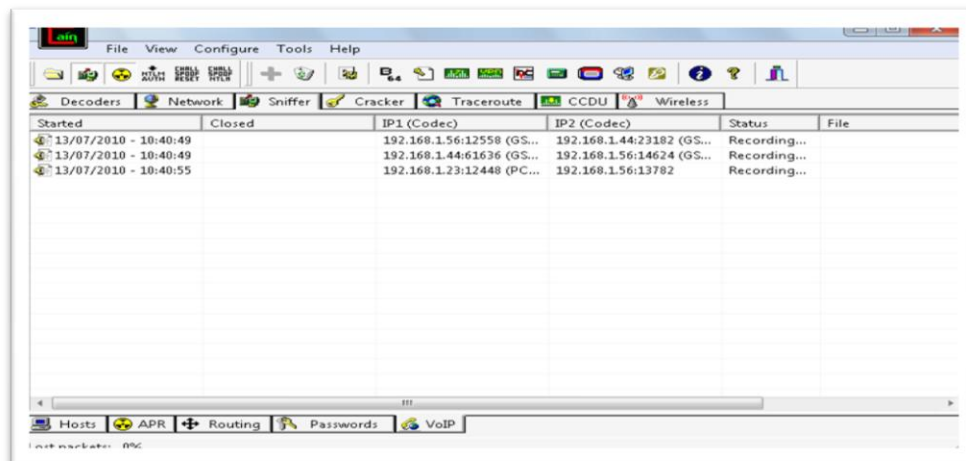
1. Pembukaan program *cain* *abel* pada *Start Menu > All Program > Cain*
2. Aktifkan proses *sniffing* dan *ARP poison routing* dengan menekan *start sniffer* dan *start poison routing* seperti pada Gambar 4.26



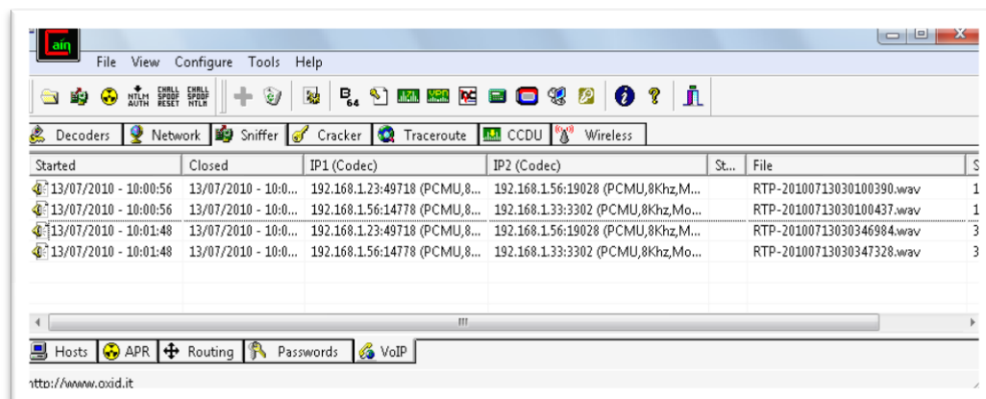
**Gambar 4.26**Menjalankan Sniffing Dan Poison Routing

3. 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.

4. 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. File yang dihasilkan dari Cain and Able adalah ber *extensikan\*.wav*. Berikut hasil *capture* dari hasil pengujian penyadapan menggunakan Cain and Able



**Gambar. 4.27** Proses Penyadapan Sewaktu Komunikasi Aktif



**Gambar. 4.28** Penyadapan Voip Setelah Sesi Komunikasi Selesai

Setelah selesai, file yang dihasilkan di simpan didalam folder dimana Cain And Able terinstal, pada windows pilih, proram files – Cain-pilih cain.exe-klik Kanan-propeties-pilih find target, (akan masuk ke folder dimana terinstal) - Pilih VoIP untuk melihat hasil penyadapan yang tersimpan.

Penanggulangan Proses penyadapan komunikasi suara pada *client 1* , *client 2* dan *server* menggunakan koneksi VPN. Disini pada VoIP *server* berperan sebagai VPN *Server*. Untuk menggunakan koneksi melalui VPN dapat dilakukan dengan langkahlangkah seperti berikut :

1. Server mengaktifkan VPN server dengan melakukan perintah `/etc/init.d/openvpn start`
2. Pada tiap-tiap *client* memiliki file *key* yang telah dibuat sebelumnya oleh VPNserver terdiri dari *ca.key client1.crt*, dan *client1.key*.
3. Pada client windows copy-kan file tersebut kedalam folder `C:/ProgramFile/OpenVPN/config`
4. Buat file baru dengan nama *client.ovpn* kemudian isikan parameter seperti berikut:

```

Client #sebagai VPN client

dev tun # device Virtual untuk VPN Client

proto udp # protokol yang digunakan untuk VPN client

remote 192.168.7.45 1194 # real IP address dari VPN server

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

cert client1.crt

key client1.key

cipher AES-128-CBC

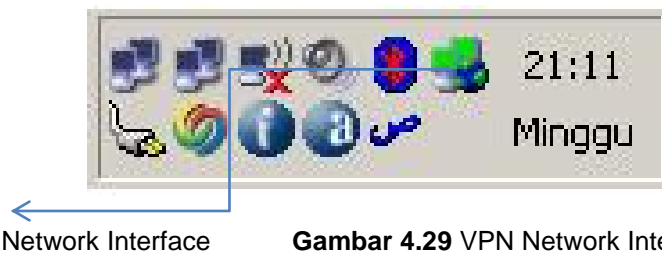
comp-lzo

verb 3

```

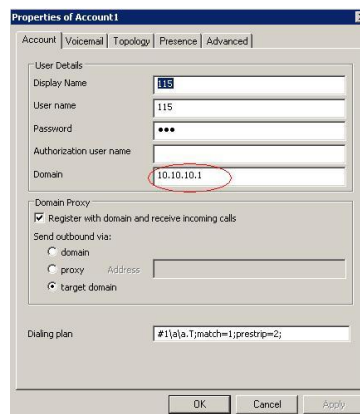
5. Pada tray icon klik kanan kemudian pilih *client1 > connect* maka koneksi VPN akan terdial dengan muncul dua buah *Network interface*. Yaitu *network interface asli* dengan *real IP address* serta *network interface virtual* dengan *virtual IPAddress* seperti pada Gambar 4.27





**Gambar 4.29** VPN Network Interface

6. Pada komputer *client* edit parameter yang terdapat pada konfigurasi VoIP client xlite > SIP Account Setting > Properties kemudian edit domain dengan mengisi IP virtual dari VPN server seperti pada Gambar 4.28



**Gambar 4.30** Memasukkan IP VPN Server Pada Voip Client

7. *Softphone VoIP Client* dilakukan perubahan *IP address domain* dengan menggunakan *virtual IP address* maka data yang dilewatkan pada jaringan akan terenkripsi oleh koneksi VPN.
8. Pengujian keamanan dilakukan kembali dengan melakukan *sniffing* untuk membuktikan bahwa jaringan menggunakan VPN bersifat lebih aman.

## BAB V

### PENUTUP

#### 5.1 Kesimpulan

Dari hasil pengujian dalam skripsi ini , dapat diambil kesimpulan sebagai berikut :

1. Penetrasyon testing pada jaringann VoIP, dengan cara memantau data VoIP yang melintas pada jaringan lokal dengan menggunakan software *Cain and Able*
2. Membangun server VoIP dengan menggunakan Server Trixbox, kemudian memberikan konfigurasi pada Server Trixbox seperti, pemberian *SIP* untuk *Client*, *Ring Group*, *Video Call*, dan Security jaringan VoIP
3. Membangun VPN dalam jaringan Lokal, sebagai jalur komunikasi antar node ( Client ke Server / Client ke Client )
4. Kemanan komunikasi didapatkan setelah terkoneksi ke *VPN Server*
5. Penggunaan VPN bersifat lebih aman dikarenakan adanya autentikasi antara server dan *client* ketika akan melakukan koneksi, serta pemberian enkripsi pada data yang akan dikirim.
6. Penggunaan VPN tidak mempengaruhi kemampuan komunikasi VoIP dalam jaringan lokal.

#### 5.2 Saran

Pada perancangan skripsi ini, penulis mencoba memberikan saran-saran untuk pengembangan dan perbaikan lebih lanjut seiring kebutuhan dan kemajuan teknologi:

1. Penggunaan VoIP merupakan solusi alternatif komunikasi masa depan, oleh karena itu untuk pengembangan selanjutnya dapat dilakukan analisis performansi VoIP dengan VoIP monitoring.
2. Sistem ini dapat dikembangkan dengan jaringan internet sehingga komunikasiakan lebih murah.
3. Pemberian aplikasi keamanan selain menggunakan VPN dapat menggunakan SRTP (*Secure Real Time Protocol*)

## DAFTAR PUSTAKA

- Dempster, Barrie, Kerry Garrison. 2006. *Trixbox Made Easy*. Birmingham – Mumbai Packt Publishing.
- Kambau, Ridwan Andi, Riswan Efendi Tarigan. 2005. *Physical Security*. Mandiri Information Systems. 2004. *Membangun Jaringan LAN (buku 5)*. Mandiri Information Systems
- Purbo, Onno W. 2007. *Cikal Bakal "Telkom Rakyat" (Paduan Lengkap Seting VoIP)*.
- Taufiq, M. 2005. *Membuat SIP Extensions Pada Linux TrixBox untuk Server VoIP*.
- Web: <http://ebas.vlsm.org/v06/Kuliah/SistemOperasi/2003/21/produk/SistemOperasi.txt> . yang berjudul "Sistem Operasi", Tanggal Unduh 28 juni 2010
- Web : [http://id.wikipedia.org/wiki/Local\\_Area\\_Network](http://id.wikipedia.org/wiki/Local_Area_Network) yang berjudul "Jaringan LAN" Tanggal Unduh : 28 juni 2010
- Web : [http://www.sony-ak.com/articles/5/network\\_security\\_beginner.php](http://www.sony-ak.com/articles/5/network_security_beginner.php) yang berjudul "Network Security Beginner", Tanggal Unduh 18 juni 2010