Jurnal Informatika dan Rekayasa Perangkat Lunak (JATIKA)
Vol. 2, No. 3, September 2021, page-page. 324~333

ISSN 2723-3367
E-ISSN 2797-3492
available online at:http://jim.teknokrat.ac.id/index.php/informatika

ANALISIS KEAMANAN VOICE OVER INTERNET PROTOCOL (VOIP) OVER VIRTUAL PRIVATE NETWORK (VPN)

Dwi Prastantio Putra
Universitas Teknokrat Indonesia

dwiprastantio_putra@teknokrat.ac.id

Published: (30 September 2021)

Abstract

This research was conducted on the basis of the influence of security systems that play a role in encrypting data on VoIP communication systems, with the security technology of PPTP VPN computer networks with the system passing data in a virtual private ip or as a tunnel for secure data transmission media. The results obtained from security analysis for the implementation of security methods on PPTP VPNs, then the data to help developers in terms of building a secure VoIP communication system. Basiclly ZRTP uses the Diffie-Hellman key exchange as a key exchange of communication between clients, which is the key for communication between clients using hashes from Diffie-Hellman and is done peer-to-peer through the VOIP RTP package, while the Point-to-Point Tunneling Protocol (PPTP) is a network protocol that allows the secure transmission of data from the remote client to the server by creating a virtual private network (VPN) through a network of data. TCP/IP or UDP is dedicated to encryption and creates RTP tunnel transport on VoIP communication systems. VoIP communication system research is conducted using 2 security methods, namely VoIP VPN PPTP, VoIP ZRTP, with the aim to find out the results of VoIP communication testing using PPTP and ZRTP VPN security methods if an attack occurs during VoIP communication.

Keywords: *Analysis VoIP, VPN PPTP, ZRTP*

Abstrak

Penelitian ini dilakukan atas dasar adanya pengaruh sistem keamanan yang berperan melakukan enkripsi data pada sistem komunikasi *VoIP*, dengan adanya teknologi keamanan jaringan komputer *VPN PPTP* dengan sistem melewatkan data dalam suatu *ip private virtual* atau sebagai *tunnel* untuk media transmisi data yang aman. Hasil yang didapat dari analisis keamanan untuk penerapan metode pengamanan pada *VPN PPTP*, lalu data tersebut untuk membantu pengembang dalam hal pembangunan sistem komunikasi *VoIP* yang aman. Pada dasarnya *ZRTP* menggunakan pertukaran kunci *Diffie-Hellman* sebagai pertukaran kunci komunikasi antar *client*, yang mana kunci untuk komunikasi antar *client* tersebut menggunakan hash dari *Diffie-Hellman* dan dilakukan secara *peer-to-peer* melalui paket *RTP VoIP*, sedangakan *Point-to-Point Tunneling Protocol (PPTP)* adalah suatu protokol jaringan yang memungkinkan pengiriman data secara aman dari remote client kepada server dengan membuat suatu *virtual private network (VPN)* melalui jaringan data berbasis *TCP/IP* atau *UDP* yang berfungsi sebagai enkripsi dan membuat *tunnel transport RTP* pada sistem komunikasi *VoIP*. Pengujian penelitian sistem komunikasi *VoIP* ini dilakukan menggunakan dengan 2 metode keamanan yaitu *VoIP VPN PPTP, VoIP ZRTP*, dengan tujuan untuk mengetahui hasil pengujian komunikasi *VoIP* dengan menggunakan metode keamanan *VPN PPTP* dan *ZRTP* apabila dilakukan penyerangan pada saat komunikasi *VoIP* berlangsung.

Kata Kunci: Analisis VoIP, VPN PPTP, ZRTP

To cite this article:
Dwi Prastantio Putra. (2021). ANALISIS KEAMANAN VOICE OVER INTERNET PROTOCOL (VOIP) OVER VIRTUAL PRIVATE NETWORK (VPN). *Jurnal Informatika dan Rekayasa Perangkat Lunak*, Vol(2) No(3), 324-333.

PENDAHULUAN

Seiring pesatnya perkembangan jumlah komputer yang saling terhubung dengan lainnya dan yang biasa disebut dengan jaringan komputer, maka munculah teknologi-teknologi baru, yaitu teknologi yang saling menghubungkan komputer di dunia, yang memungkinkan untuk dapat saling bertukar informasi dan data (Megawaty et al., 2021), bahkan dapat saling berkomunikasi dan bertukar informasi berupa gambar atau *video* (I. Kurniawan et al., 2020). Perkembangan jaringan komputer yang semakin pesat memungkinkan untuk melewatkan trafik suara melalui jaringan komputer atau yang biasa disebut *VoIP (Voice Over Internet Protocol*).

Teknologi *(Voice Over Internet Protocol) VoIP* merupakan teknologi yang menawarkan layanan transmisi data suara secara langsung *(real time)* dengan menggunakan *Internet Protocol* (Amarudin et al., 2014; Amarudin & Riskiono, 2019). Akan tetapi komunikasi *VoIP* tidak memiliki jaminan keamanan terhadap data pada komunikasi suara yang sedang berlangsung, tidak menutup kemungkinan pihak lain yang tidak berwenang melakukan penyadapan terhadap komunikasi tersebut, seperti : pembajakan terhadap isi data *(sniffing)* ataupun tidak dapat mengakses *server* dikarenakan *server* kelebihan muatan *(denial of service)*.

Penanggulangan dari beberapa hal tersebut adalah dengan pengimplementasian metode keamanan data terhadap layanan *VoIP*, diantaranya dengan implementasi keamanan protokol *VPN PPTP* dan *ZRTP (Zimmermann Real Time Transport Protocol)* (Amarudin & Ulum, 2018; Napianto et al., 2017). *VPN* merupakan jaringan *public* yang menekankan pada keamanan data dan akses global melalui *internet*. Penggunaan *Virtual Private Network (VPN)* merupakan salah satu alternatif untuk mengirimkan *voice*, yang bersifat *private* atau aman, karena penggunaan koneksi yang telah terenkripsi serta penggunaan *private keys*, *certificate, username* atau *password* untuk melakukan authentikasi dalam membangun koneksi. *ZRTP (Zimmermann Real-Time Transport Protocol)* menghasilkan *shared secret* antara *initiator* dan *responder* yang kemudian digunakan untuk menghasilkan kunci *Secure RTP (SRTP). ZRTP* menggunakan pertukaran kunci *Diffie-Hellman* yang menegosiasikan kunci untuk mengenkripsi suara pada komunikasi *VoIP*. Pertukaran kunci tersebut yang akan menjaga suara atau komunikasi yang sedang berlangsung dari serangan pada komunikasi *VoIP*. Sehingga enkripsi yang dihasilkan adalah *end to end* antara pemanggil dan penerima (Amarudin et al., 2014; F. Kurniawan & Surahman, 2021).

Berdasarkan latar belakang diatas penulis mecoba untuk melakukan pengujian komunikasi *VoIP* dengan menggunakan metode keamanan *VPN PPTP* dan *ZRTP* untuk meminimalisir terjadinya penyadapan, dengan tujuan untuk mengetahui hasil pengujian komunikasi *VoIP* dengan menggunakan metode keamanan *VPN PPTP* dan *ZRTP* apabila dilakukan penyerangan pada saat komunikasi *VoIP* berlangsung.

Analisa Perancangan *Server VoIP (Voice Internet Protocol)* Dengan *Opensource Asterisk* Dan *VPN (Virtual Private Network)* Sebagai Pengaman Jaringan Antar *Client"*. Melakukan pengujian layanan *VoIP* dengan cara penyadapan melalui software cain and abel, sekenario penyadapan adalah saat client 1 berkomunikasi dengan client 2, maka computer 3 melakukan penyadapan, hasilnya terbukti dengan menggunakan software cain and abel, saat client sedang berkomunikasi, computer 3 dapat mencapture 117 *protocol SIP*. Melakukan pengujian *QoS* diantaranya *delay* dan *throughput* (Yuniati et al., 2014).

Perbandingan Performa Dan Keamanan *Voice Over Internet Protocol* Dengan Dan Tanpa *Open Virtual Private Network* (Studi Kasus Kos Gayam)". Hasil dari penelitian adalah Pengujian *delay VoIP* tanpa *Open VPN* pada saat jaringan tidak sibuk mencapai 0,000441s dan pada saat jaringan sibuk mencapai 0,000363s. Sedangkan *VoIP* dengan *Open VPN* pada saat jaringan tidak sibuk mencapai 0,00046s dan pada saat jaringan sibuk mencapai 0,00032s. Pengujian performa beban *network VoIP* tanpa *Open VPN* pada saat jaringan tidak sibuk mencapai 0,37% dan pada saat jaringan sibuk mencapai 22,25%. Sedangkan untuk *VoIP* dengan *Open VPN* dalam pengujian performa beban *network*, pada saat jaringan sibuk maupun tidak sibuk, tetap stabil mencapai 1,71%.Sistem *VoIP Open VPN* jauh lebih aman dibandingkan sistem *VoIP* tanpa *Open VPN* karena tidak dapat disadap (Yulkarnain et al., 2013).

METODE PENELITIAN

Objek Penelitian

Penelitian ini akan dilakukan pada sebuah *PC* yang dibangun sebagai *VoIP server*, satu unit *router* sebagai penghubung antar jaringan, satu unit *switch* sebagai sentral penghubung *node* jaringan, dan 3unit laptop sebagai *VoIP client*. Sistem komunikasi *VoIP* yang akan dibangun tersebut terdapat 2 jenis, sistem komunikasi *VoIP* dengan pengujian menggunakan *VPN PPTP, ZRTP* tanpa *VoIP* tanpa keamanan, yang kemudian nantinya akan dilakukan uji keamanan terhadap data suara *(voice)*.

Analisa akan dilakukan dengan membandingkan keamanan yang dihasilkan pada *VoIP VPN PPTP, ZRTP* dan *VoIP* tanpa keamanan. Kemudian dilakukan perbandingan terhadap data yang diperoleh ketika melakukan analisa dari komunikasi *VoIP* tersebut.

Teknik Pengumpulan Data

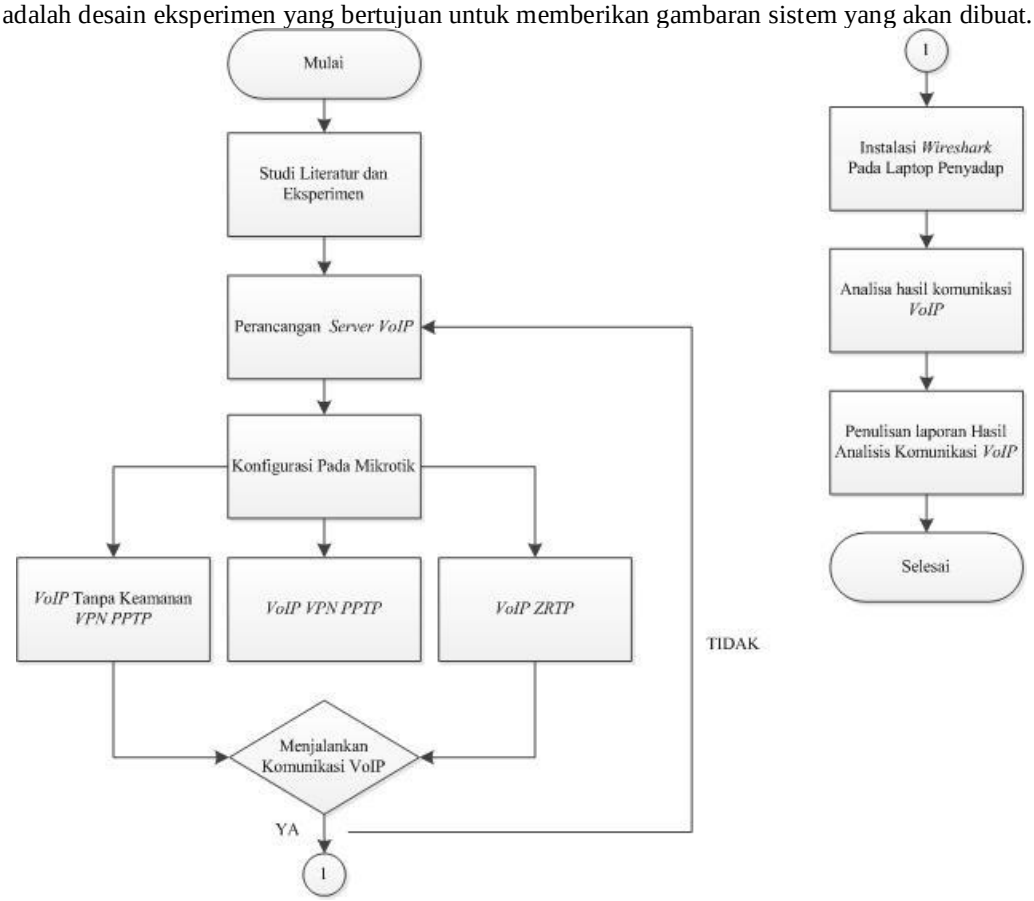
Pengumpulan data yang dilakukan pada penelitian ini adalah sebagai berikut:

1. Studi Literatur.
   Pengumpulan data yang diperoleh melalui *literature*, melakukan studi kepustakaan dengan cara membaca jurnal, membaca buku dan membaca bahan bacaan di internet yang berkaitan sesuai dengan objek serta parameter yang sedang diteliti (Setiawansyah et al., 2021; Sulistiani et al., 2021).
2. Eksperimen
   Pengumpulan data yang dilakukan dengan cara melakukan percobaan terhadap suatu hal, yang dilanjutkan dengan melakukan pengamatan dan pencatatan terhadap yang berkaitan dengan penelitian (Darwis et al., 2020; Rusliyawati et al., 2020; Yana et al., 2020).

HASIL DAN PEMBAHASAN

Desain Ekperimen

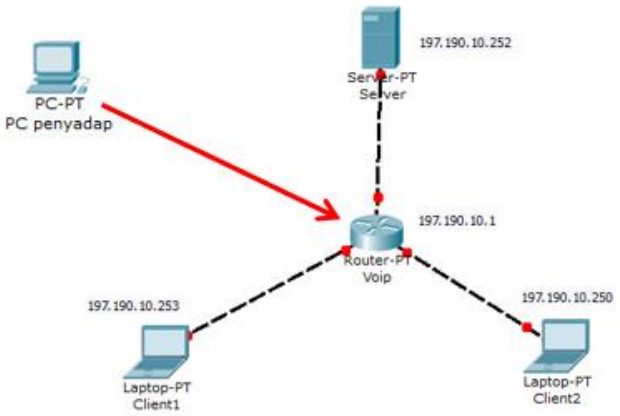
Pada rancangan ini akan dibuat sistem untuk berkomunikasi secara aman dari sisi penyadapan, oleh klarena itu pada laporan ini penulis mencoba membangun *Voice Over Internet Protocol* (*VoIP*) *over Virtual Private Network* (*VPN*), yaitu dengan membangun *VoIP* yang merupakan sistem komunikasi dengan melalui jalur *VPN PPTP* yang memberikan keamanan dan integritas data serta fungsionalitas yang mendukung untuk mengamankan jalur komunikasi suara pada *VoIP* (Budiman et al., 2019; Riskiono, 2018; Supriyatno et al., 2020). Berikut adalah desain eksperimen yang bertujuan untuk memberikan gambaran sistem yang akan dibuat.



Gambar 1. Desain Sistem Pengujian *VoIP*

Perancangan Topologi

Perancangan topologi dibuat untuk memberikan gambaran topologi yang akan dijalankan untuk proses pengujian



Gambar 2. Desain Topologi

Pembangunan VoIP Server

VoIP server adalah komputer yang menyediakan layanan *VoIP*. *VoIP server* yang digunakan yaitu *Asterisk* yang berjalan pada sistem operasi *Ubuntu 12.04 LTS*. Kebutuhan *hardware* dari *VoIP server* adalah sebagai berikut:

Tabel 1. Spesifikasi *Hardware VoIP Server*

Perangkat Keras	Spesifikasi
Processor	*1.6*
Memory	*4 GB*
Harddisk	*250 GB*
Operating System	*Ubuntu 16.04 LTS*
Ethernet	✓
Mouse	✓
Keyboard	✓
Monitor	✓

Implementasi VoIP Client

Komputer *client* dapat menggunakan layanan *VoIP* melalui aplikasi *VoIP client*. Aplikasi *VoIP client* yang digunakan adalah *phonerlite* versi 2.42. Spesifikasi dari perangkat keras yang digunakan yaitu:

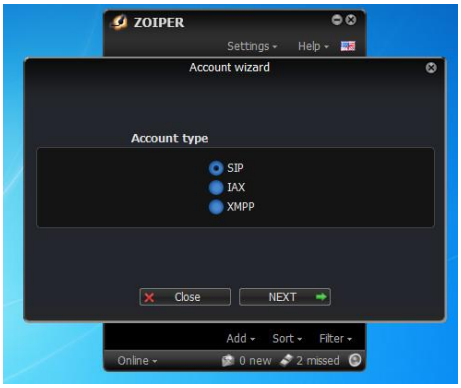
Tabel 2. Kebutuhan Perangkat Keras *Client*

Hardware	Spesification
Processor	2,20 *GHz*
Memory	2048 *MB*
Harddisk	500 *GB*
Operating System	*Windows 7 Ultimate*
Audio Microphone / Speaker	✓

Membuat Account pada Zoiper

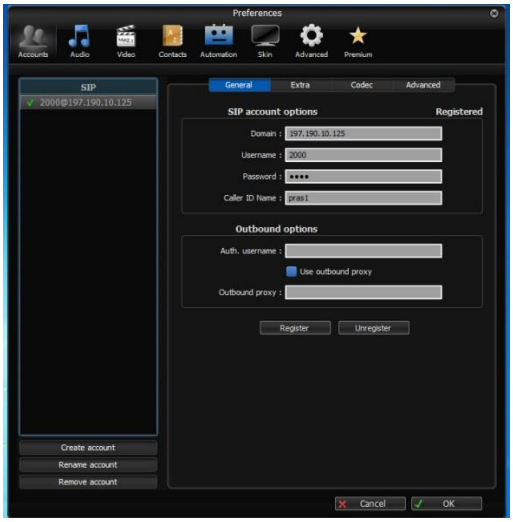
SIP ID yang telah dikonfigurasi pada *server VoIP* lalu diimplementasikan pada *VoIP client*. Berikut adalah langkah untuk mengimplementasikan *SIP ID user* pras1 pada *client* :

1. Pada aplikasi *Zoiper*, pilih new account dan *account type* lalu pilih SIP



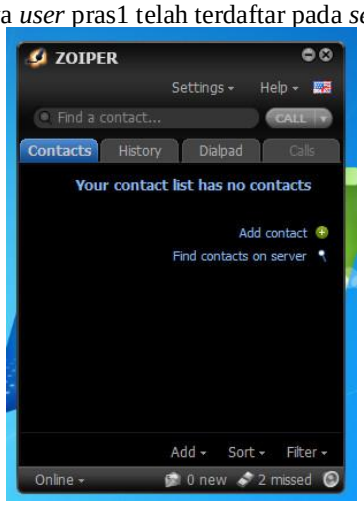
Gambar 1. *Account Type*

2. Kemudian isikan pada bagian Account seperti *username* dan *caller id*, isikan extensions dan id sesuai dengan yang telah dikonfigurasi pada *file sip.conf* dan *extensions.conf* pada *server VoIP* sebelumnya, kemudian *klik* ok.



Gambar 2. Konfigurasi *Account Zoiper*

3. Setelah *SIP ID* telah berhasil diimplementasikan akan muncul tanda pemberitahuan "*Online"* pada bagian bawah yang menyatakan bahwa *user* pras1 telah terdaftar pada *server* 197.190.1.125



Gambar 3. *Account Zoiper* Berstatus *Online*

4. Setelah semua konfigurasi telah selesai, lalu mencoba melakukan panggilan antar *client*

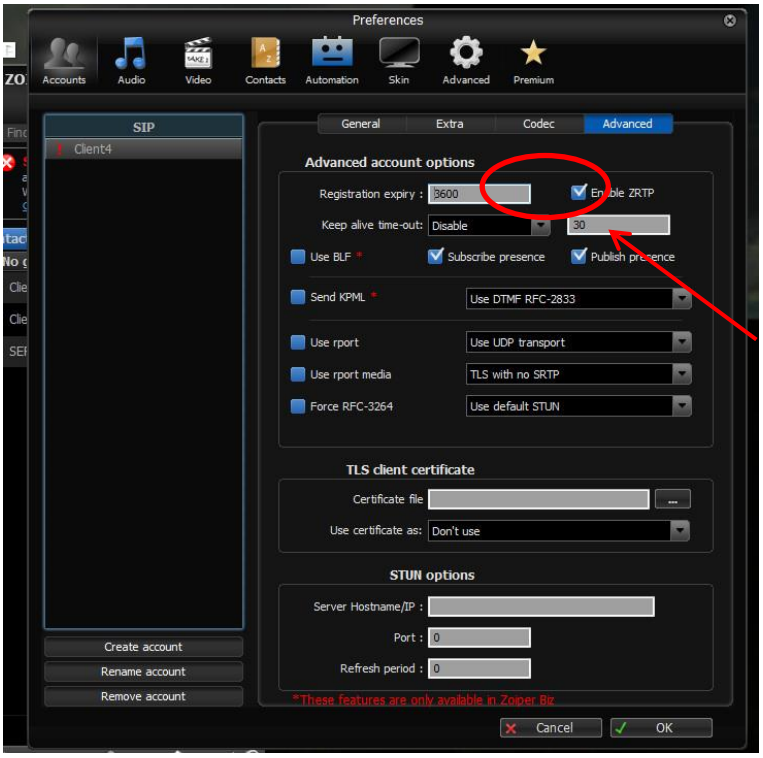
Gambar 4. Proses *Dial*

Gambar 5. Proses *Incoming Call*

Konfigurasi ZRTP

Komunikasi *VoIP* dengan *ZRTP* dapat dilakukan ketika *VoIP server* dan *VoIP client* telah mendukung. Protokol *ZRTP* sudah didukung oleh aplikasi *ZOIPER* tanpa memerlukan konfigurasi tambahan. Pada sisi *VoIP Client* yang menggunakan *ZOIPER*, diperlukan konfigurasi untuk mendukung protokol *ZRTP* pada komunikasi *VoIP* dengan langkah sebagai berikut:

1. Pilih menu *Settings*, lalu *tab Accounts*, pilih menu *advanced* dan ceklis *enable ZRTP* yang akan digunakan untuk keamanan pada komunikasi *VoIP* di aplikasi *ZOIPER*.
2. Setelah ceklis pada tab *Enable ZRTP* seperti gambar berikut, lalu klik *icon OK* untuk menyimpan konfigurasi.



Gambar 6. Konfigurasi *ZRTP VoIP Client*

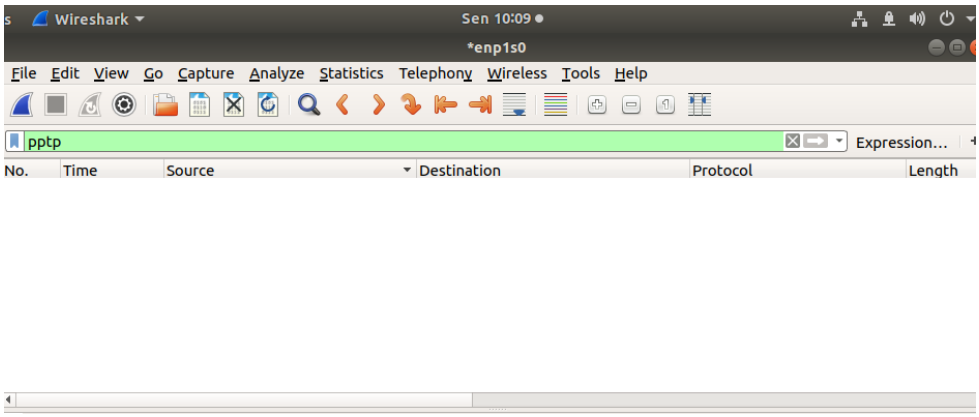
Pengujian Keamanan VoIP VPN PPTP

Pada skenario ini dilakukan pengujian sebelum komunikasi *VoIP* berlangsung pada dasarnya sama seperti pengujian sebelumnya. Untuk langkah mengaktifkan mode keamanan *VPN PPTP* dan penyadapan pada *VoIP client* dapat dijelaskan seperti berikut:

1. Koneksikan laptop *client* dalam mode jaringan *VPN PPTP*, hubungkan *VPN PPTP* pada *notification area*, lalu klik *connect*, masukkan *username* serta *password* seperti yang telah dibuat pada *VPN PPTP server* pada *mikrotik.* Tunggu proses *verifying username* and *password* selesai, kemudian terkoneksi seperti gambar dibawah ini.

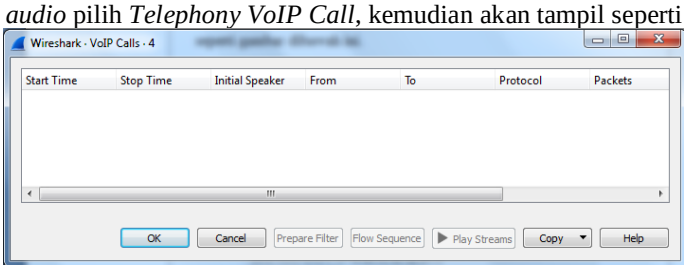
Gambar 7. *Client VPN PPTP Connected*

2. Setelah itu lakukan panggilan antar *user* Client1 dengan Client2 seperti pengujian yang dilakukan sebelumnya.
3. Kemudian setelah *wireshark* dari laptop *attacker* menangkap paket dari komunikasi tersebut, maka akan terlihat paket *RTP* seperti gambar dibawah ini.



Gambar 8. Paket *VPN PPTP*

4. Untuk melihat *stream audio* pilih *Telephony VoIP Call*, kemudian akan tampil seperti gambar dibawah ini.



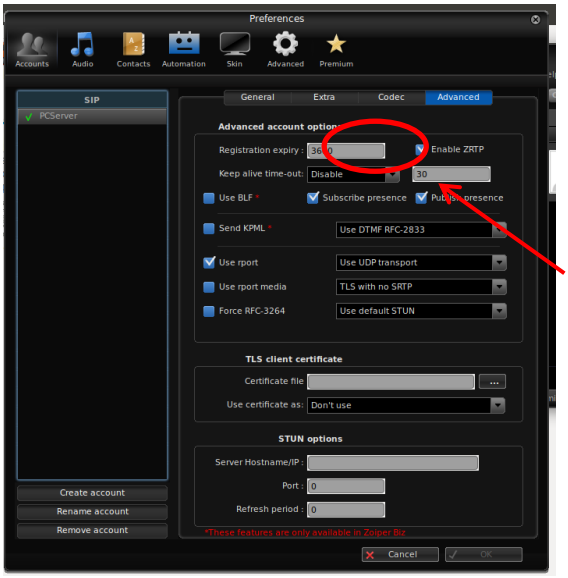
Gambar 9. Deteksi Komunikasi *VoIP VPN PPTP*

5. Pada tampilan tersebut tidak ada komunikasi *VoIP* yang terdeteksi, jadi *SIP* tidak terdeteksi.

Pengujian Keamanan VoIP ZRTP

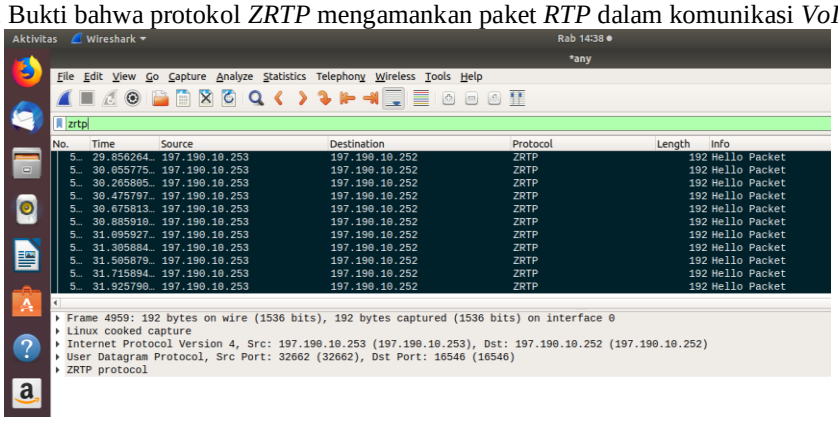
Pada skenario ini dilakukan pengujian sebelum komunikasi *VoIP* berlangsung pada dasarnya sama seperti pengujian sebelumnya. Untuk langkah mengaktifkan mode keamanan *ZRTP* dan penyadapan pada *VoIP client* dapat dijelaskan seperti berikut:

1. Aktifkan mode *ZRTP* pada aplikasi *zoiper user client*1 dan *client*2, lalu mulai komunikasi antar *user* seperti skenario sebelumnya. Untuk mengaktifkan mode *ZRTP* dapat dilihat seperti gambar dibawah, ceklist *ZRTP* lalu *ok*.



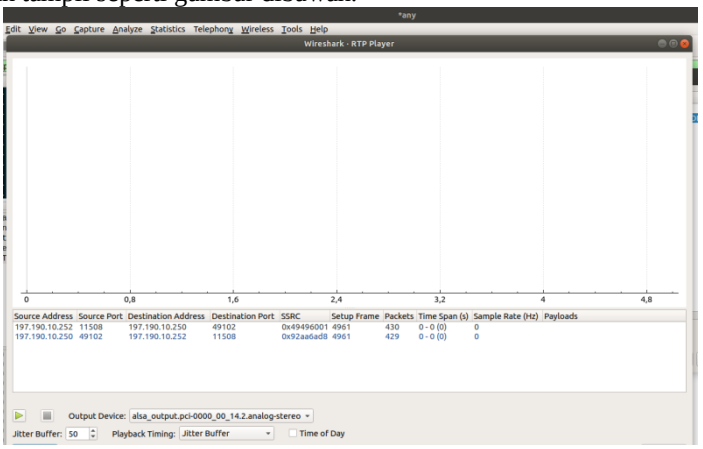
Gambar 10. *ZRTP* Pada *ZOIPER*

2. Pada penyadapan *wireshark* akan tampil *file RTP* yang dilindungi oleh protokol *ZRTP*, seperti gambar dibawah ini. Bukti bahwa protokol *ZRTP* mengamankan paket *RTP* dalam komunikasi *VoIP*.



Gambar 11. Komunikasi *ZRTP* Pada *Wireshark*

3. Untuk membuktikan keamanan *ZRTP* pada *RTP*, pilih menu *Telephony* kemudian pilih *VoIP Call*, kemudian *Play Streams*. Akan tampil seperti gambar dibawah.



Gambar 12. Deteksi Komunikasi *ZRTP*

4. Untuk mendengarkan *audio* dari *RTP Stream* tersebut klik *icon play*.
5. *Audio* percakapan antar *user client*1 dengan *client*2 tidak dapat didengarkan.

SIMPULAN

Setelah melakukan serangkaian implementasi pembangunan *VoIP* dan pengujian dengan skenario yang telah dijelaskan pada bab sebelumnya, maka dapat disimpulkan sebagai berikut Sistem komunikasi *VoIP* tanpa keamanan apabila diserang dapat mengetahui hasil komunikasi yang sedang berlangsung dan di *capture* hasil suara berdasarkan *VoIP Call Detect* dan *RTP Player*. Sistem komunikasi *VoIP VPN PPTP* apabila diserang tidak dapat mengetahui hasil komunikasi yang sedang berlangsung dan di *capture* hasil suara berdasarkan *VoIP Call Detect* dan *RTP Player*. Sistem komunikasi *VoIP ZRTP* apabila diserang dapat mengetahui hasil komunikasi yang sedang berlangsung dan tetapi tidak dapat di *capture* hasil suara berdasarkan *RTP Player*

REFERENSI/DAFTAR PUSTAKA

Amarudin, A., & Riskiono, S. D. (2019). Analisis Dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (Vpn). *Jurnal Teknoinfo*, *13*(2), 100–106.

Amarudin, A., & Ulum, F. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port

Knocking. *Jurnal Teknoinfo*, *12*(2), 72–75.
Amarudin, A., Widyawan, W., & Najib, W. (2014). Analisis Keamanan Jaringan Single Sign On (SSO) Dengan Lightweight Directory Access Protocol (LDAP) Menggunakan Metode MITMA. *SEMNASTEKNOMEDIA ONLINE*, *2*(1), 1–7.
Budiman, A., Samsugi, S., & Indarto, H. (2019). SIMULASI PERBANDINGAN DYNAMIC ROUTING PROTOCOL OSPF PADA ROUTER MIKROTIK DAN ROUTER CISCO MENGGUNAKAN GNS3 UNTUK MENGETAHUI QOS TERBAIK. *Seminar Nasional Teknik Elektro*, *4*(1), 16–20.
Darwis, D., Ferico Octaviansyah, A., Sulistiani, H., & Putra, R. (2020). Aplikasi Sistem Informasi Geografis Pencarian Puskesmas Di Kabupaten Lampung Timur. *Jurnal Komputer Dan Informatika*, *15*(1), 159–170.
Kurniawan, F., & Surahman, A. (2021). SISTEM KEAMANAN PADA PERLINTASAN KERETA API MENGUNAKAN SENSOR INFRARED BERBASIS MIKROKONTROLLER ARDUINO UNO. *Jurnal Teknologi Dan Sistem Tertanam*, *2*(1), 7–12.
Kurniawan, I., Setiawansyah, & Nuralia. (2020). PEMANFAATAN TEKNOLOGI AUGMENTED REALITY UNTUK PENGENALAN PAHLAWAN INDONESIA DENGAN MARKER. *Jurnal Informatika Dan Rekayasa Perangkat Lunak*, *1*(1), 9–16.
Megawaty, D. A., Setiawansyah, S., Alita, D., & Dewi, P. S. (2021). Teknologi dalam pengelolaan administrasi keuangan komite sekolah untuk meningkatkan transparansi keuangan. *Riau Journal of Empowerment*, *4*(2), 95–104.
Napianto, R., Utami, E., & Sudarmawan, S. (2017). VIRTUAL PRIVATE NETWORK (VPN) PADA SISTEM OPERASI WINDOWS SERVER SEBAGAI SISTEM PENGIRIMAN DATA PERUSAHAAN MELALUI JARINGAN PUBLIK (STUDI KASUS: JARINGAN TOMATO DIGITAL PRINTING). *Respati*, *7*(20).
Riskiono, S. D. (2018). Implementasi Metode Load Balancing Dalam Mendukung Sistem Kluster Server. *SEMNAS RISTEK*, 455–460.
Rusliyawati, R., Damayanti, D., & Prawira, S. N. (2020). IMPLEMENTASI METODE SAW DALAM SISTEM PENDUKUNG KEPUTUSAN PEMILIHAN MODEL SOCIAL CUSTOMER RELATIONSHIP MANAGEMENT. *Edutic-Scientific Journal of Informatics Education*, *7*(1).
Setiawansyah, S., Adrian, Q. J., & Devija, R. N. (2021). Penerapan Sistem Informasi Administrasi Perpustakaan Menggunakan Model Desain User Experience. *Jurnal Manajemen Informatika (JAMIKA)*, *11*(1), 24–36.
Sulistiani, H., Sulistiyawati, A., & Hajizah, A. (2021). Perancangan Sistem Pengelolaan Keuangan Komite Menggunakan Web Engineering (Studi Kasus: SMK Negeri 1 Gedong Tataan). *Komputika: Jurnal Sistem Komputer*, *10*(2), 163–171.
Supriyatno, S., Jupriyadi, J., Ahdan, S., & Riskiono, S. D. (2020). PERBANDINGAN KINERJA RIP DAN OSPF PADA TOPOLOGI MESH MENGGUNAKAN CISCO PACKET TRACER. *TELEFORTECH: Journal of Telematics and Information Technology*, *1*(1), 1–8.
Yana, S., Gunawan, R. D., & Budiman, A. (2020). SISTEM INFORMASI PELAYANAN DISTRIBUSI KEUANGAN DESA UNTUK PEMBANGUNAN (STUDY KASUS: DUSUN SRIKAYA). *Jurnal Informatika Dan Rekayasa Perangkat Lunak*, *1*(2), 254–263.
Yulkarnain, D., Raharjo, S., & Lestari, U. (2013). PERBANDINGAN PERFORMA DAN KEAMANAN VOICE OVER INTERNET PROTOKOL DENGAN DAN TANPA OPEN VIRTUAL PRIVATE NETWORK (STUDI KASUS KOS GAYAM). *Jurnal Jarkom*, *1*(1).
Yuniati, Y., Fitriawan, H., & Patih, D. F. J. (2014). Analisa Perancangan Server VoIP (Voice Internet Protocol) dengan Opensource Asterisk dan VPN (Virtual Private Network) Sebagai Pengaman Jaringan Antar Client. *Jurnal Sains, Teknologi Dan Industri*, *12*(1), 112–121.