UM Jember Proceeding Series
National Multidisciplinary Sciences **(2022)** Vol. 1 No 6 : 857-870

SENSEI 2021

Analisis Kualitas Layanan Pada Jaringan Voip Menggunakan Jaringan Virtual Pribadi Sebagai Mekanisme Pengamanan Jaringan

M.Fatkhur Rohman[1*], Triawan Adi Cahyanto[1]
[1]Universitas Muhammadiyah Jember
email: aefatur@gmail.com

DOI: https://doi.org/10.32528/nms.v1i6.243
*Correspondensi: M.Fatkhur Rohman
Email: aefatur@gmail.com

Published: November, 2022

Abstrak: Teknologi internet terus berkembang, saat ini pemanfaatan teknologi internet lebih banyak digunakan sebagai hiburan, walaupun pada dasarnya teknologi internet memiliki manfaat yang banyak, seperti; pemanfaatan berbagai macam aplikasi yang berguna diberbagai disiplin ilmu atau bidang. Salah satunya pemanfatan teknologi internet adalah teknologi VoIP (Voice over Internet Protocol). Kualitas suara pada teknologi VoIP sangat dipengaruhi oleh Quality of Service (QoS) dan apabila paket dari voice mengalami proses yang lama (delay) untuk sampai ke tujuan, maka dapat merusak kualitas voice yang terdengar. Selain itu dari segi keamanan saat melakukan komunikasi, teknologi VoIP masih tergolong kurang baik. Pada penelitian ini telah dilakukan riset tentang analisis kualitas layanan pada jaringan VoIP dengan parameter delay, Throughput dan packet loss. Sedangkan mekanisme pengamanan jaringan VoIP pada penelitian ini menggunakan protokol VPN. Hasil analisis nilai QoS dengan 6 kali pengujian rentang waktu 1-6 menit diperoleh nilai rata-rata Delay 7,758 ms, 7,657 ms, dan 299 bps, 210 bps, dan Packet loss 0%. Analisis keamanan VoIP dengan menggunakan dua skenario pengujian diperoleh data VoIP antara dua client yang sama-sama terhubung dengan VPN Attacker, dimana hanya dapat melakukan scan IP dan Mac address saja, namun tidak dapat merekam atau mendengarkan percakapan antara client yang saling komunikasi. Skenario kedua client terhubung dengan VPN Attacker dapat melakukan scan IP dan Mac Address, selain itu Attacker dapat merekam atau mendengarkan percakapan antara dua client dalam waktu singkat.

Keywords: *VoIP, VPN, QoS, Delay, Throughput, Packet loss.*

PENDAHULUAN

Teknologi internet terus berkembang selaras juga dengan pemanfaatan teknologi yang mayoritas masih sebatas penggunaan untuk hiburan, namun di sisi lain teknologi ini bisa dimanfaatkan untuk aplikasi yang berguna. Salah satu pemanfatan teknologi internet adalah penggunaan teknologi VoIP (*Voice Over Internet Protocol*). VoIP adalah teknologi yang memungkinkan percakapan suara melalui media jaringan komputer (Patih, 2012). VoIP menawarkan alternatif komunikasi yang berbeda dengan komunikasi telepon tradisional. Salah satu perbedaan telepon tradisional dengan VoIP adalah pada infrastrukturnya. Jika VoIP saat penggunaan untuk komunikasi menggunakan teknologi internet, sedangkan telepon tradisional menggunakan infrastruktur yang dibangun oleh perusahaan telepon konvensional (Sugeng, 2008). Meskipun saat ini komunikasi jarak jauh bisa menggunakan telepon tradisional, tetapi panggilan telepon di Indonesia biayanya masih relatif mahal (Sutarti, dkk., 2018). Apalagi jika jaraknya antar negara yang berbeda, maka semakin mahal pula biaya yang di perlukan untuk berkomunikasi. Seiring dengan berkembangnya teknologi jaringan internet, permasalahan tersebut dapat diatasi, salah satunya dengan memanfaatkan VoIP (*Voice over Internet Protocol*). Terdapat kekurangan pada VoIP yaitu kualitas suara sangat dipengaruhi oleh *Quality of*

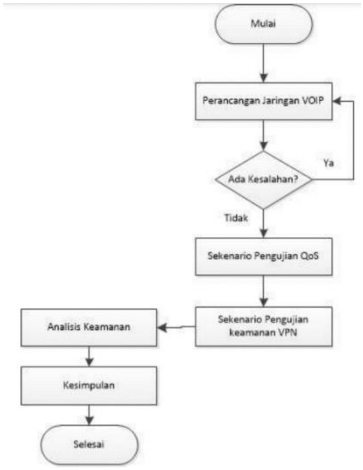
Service (QoS) yang dapat diukur dari tiga pendekatan, yaitu *delay*, *throughput* dan *packet loss*. Apabila paket dari *voice* mengalami proses yang lama (*delay*) untuk sampai ke tujuan, maka dapat merusak kualitas *voice* yang terdengar. Selain itu, besarnya *throughput* dan *packet loss* juga berpengaruh terhadap kualitas dari VoIP itu sendiri (Setiawan, E.B., 2012).

Berdasarkan uraian diatas, maka penelitian ini akan membahas bagaimana menerapkan teknologi VoIP untuk mengatasi permasalahan tingkat ukur kualitas layanan berdasarkan ketiga parameter yang sudah ditentukan. Selain itu, penelitian terkait perancangan arsitektur jaringan menggunakan teknologi VoIP yang dapat digunakan untuk berkomunikasi sebagai telepon yang umum digunakan masih relevan untuk diterapkan. Teknologi VoIP diharapkan dapat menjadi langkah awal untuk menerapkan teknologi komunikasi yang dapat diintegrasikan dengan jaringan lokal dan dapat mengelola sendiri sarana & prasarana komunikasinya, serta kualitas suara dapat diperoleh dengan mengukur tiga parameter yaitu *delay*, *throughput*, dan *packet loss* diharapkan dapat mengetahui tingkat kualitas suara yang dihasilkan saat *client* melakukan komunikasi.

Teknologi VoIP bersifat *free* atau tidak berbayar, hal ini sangat menguntungkan bagi penggunanya. Namun, penggunaan komunikasi yang murah dari segi keamanan kurang begitu diperhatikan (Laurentinus, 2015; Winarno, N., & Cahyanto, T., 2021). Oleh karena itu, keamanan saat melakukan komunikasi suara merupakan suatu hal yang sangat penting (Amarudin, dkk., 2014; Cahyanto, T. A., Oktavianto, H., & Royan, A. W, 2016). Banyak sekali ancaman serangan yang dapat dilakukan, misal penyadapan, pengalihan aliran komunikasi, dan bahkan membajak panggilan VoIP. Salah satu serangan yang mengancam protokol dan sistem VoIP adalah serangan MITM (*Man in the Middle Attack*). MITM merupakan suatu serangan yang dimana *attacker* berada diantara kedua belah pihak yang sedang berkomunikasi sehingga bebas mendengarkan percakapan antara dua pihak tersebut (Yaqin, M. A., Cahyanto, T. A., & Fitriyah, N. Q., 2021). Maka dari itu untuk mengatasi serangan MITM di jaringan VoIP, diperlukan VPN (*Virtual Private Network*) sebagai mekanisme pengamanan lalu lintas data pada jaringan.

METODE PENELITIAN

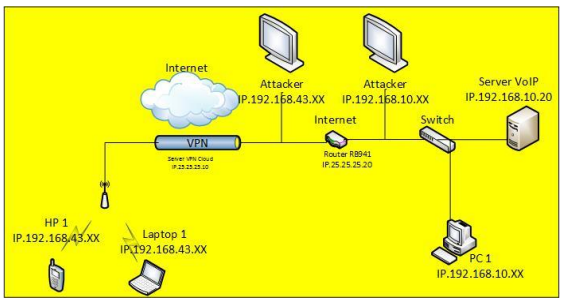
Metode penelitian adalah suatu mekanisme untuk mendapatkan data yang akan digunakan untuk keperluan penelitian. Metode penelitian dalam pengerjaan penelitian ini sudah sesuai dengan rencana topik yang dikerjakan. Berikut ini merupakan diagram alur penelitian:



Gambar 1. Diagram Alur Penelitian [Sumber: Laurentinus, 2015]

a. Perancangan Topologi VOIP

Pada perancangan Topologi VoIP ini ada beberapa komponen yang di gunakan untuk mendukung penelitian ini agar berjalan dengan lancar seperti apa yang di inginkan oleh peneliti, yaitu: *Komputer Client, Server, Smartphone, Switch, Wireless, Router RB941, Router Cloud.* Perancangan arsitektur jaringan akan membahas topologi jaringan yang dibuat dan di konfigurasi yang meliputi *device-device* yang akan digunakan terkait konektivitas antar server VoIP dengan device lainnya. Berikut rancangan topologi VoIP yang akan dibuat:



Gambar 2. Topologi Jaringan

b. Implementasi VOIP

Alat dan bahan yang digunakan pada penelitian ini adalah Sistem Operasi *Windows & Linux* sebagai *client, software trixbox* sebagai server, *sistem* VPN PPTP sebagai keamanan jaringan, *wireshark* sebagai tool pengukur *performa* kualitas jaringan VoIP dengan menganalisis QoS, *Softphone* sebagai aplikasi telpon yang di *install* di *client, cain and abel* sebagai *tool* penguji keamanan jaringan VoIP.

Pada penelitian ini telah dilakukan pengukuran terhadap parameter QoS yang mempengaruhi kualitas suara saat VoIP melakukan komunikasi yaitu, *Delay, Throughput, Packet loss* dan pengukuran kualitas keamanan VPN dari serangan MITM pada jaringan VoIP.

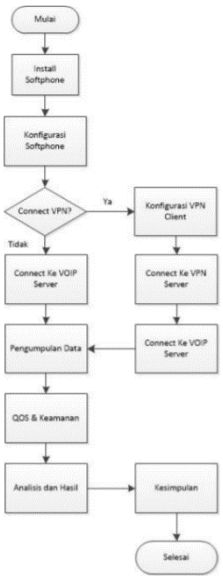
Adapun skema pengujian yang dilakukan pada penelitian ini adalah sebagai berikut:

1. Laptop 1 melakukan panggilan kepada HP 1 selama 6 kali pemanggilan dengan rentang waktu 1 – 6 menit
2. PC 1 melakukan panggilan kepada HP 1 selama 6 kali pemanggilan dengan rentang waktu 1 – 6 menit

3. Mencari nilai kualitas jaringan VoIP dengan QOS, parameter yang digunakan *Delay*, *Throughput*, *Packet loss*, dengan menggunakan *tool quality monitoring* yaitu *Wireshark*, selama 6 kali proses pemanggilan dengan rentang waktu 1-6 menit.
4. PC *Attacker* melakukan *attacking* bertindak sebagai MITMA (*Man In The Middle Attack* dengan menjalankan program *sniffer* atau *spoofing*, terhadap *client* yang sedang melakukan komunikasi, *Attacking* berada di tengah-tengah *client* yang berkomunikasi, dengan menggunakan *tool cain* and *abel*.

c. Perancangan Analisis Nilai QoS dan Keamanan VoIP

Perancangan ini dibutuhkan untuk mengatahui kualitas Nilai QoS dan keamanan jaringan VoIP dengan menggunakan VPN



Gambar 3. Perancangan Konfigurasi *Client* dan Analisis Penelitian [Sumber: Laurentinus, 2015]

d. Pengujian dan Analisis

Pada penelitian ini diuji pula koneksi antar *client* yang saling terhubung. Pengujian di lakukan sebanyak 6 kali, untuk meningkatkan akurasi, pengamatan dan pengambilan data. Pada tahap ini akan melakukan analisis jaringan VoIP, analisis pengujian dilakukan dengan cara melakukan pengukuran parameter *delay*, *Throughput dan packet loss* dengan menggunakan *Wireshark* sebagai *network analizer*.

1. *Delay*

   Pengujian parameter *Delay* dilakukan untuk mengetahui kualitas nilai QoS, semakin rendah nilai *Delay* yang diperoleh maka bisa dinilai sangat baik. Begitu juga sebaliknya semakin tinggi nilai *Delay* yang diperoleh, maka kualitas sangat buruk. Proses pengujian ini di lakukan dengan 6 kali percobaan panggilan, dengan rentang waktu 1 – 6 menit. Percobaan pertama Laptop1 melakukan panggilan pada HP1 selama 1 -6 menit, percobaan ke dua PC1 melakukan panggilan pada HP1 selama 1 – 6 menit, kemudian ditahap akhir di cari nilai rata-rata dari 6 kali percobaan tersebut.

2. *Throughput*

Pengujian parameter *throughput* dilakukan untuk mengetahui nilai kecepatan rata-rata dari sebuah paket data yang dikirim. Semakin rendah nilai *throughput* yang diperoleh maka dinilai kualitas buruk, begitu juga sebaliknya semakin tinggi nilai *throughput* yang diperoleh maka kualitas sangat baik. Proses pengujian ini di lakukan dengan 6 kali percobaan panggilan, dengan rentang waktu 1-6 menit. Percobaan pertama Laptop1 melakukan panggilan pada HP1 selama 1-6 menit, percobaan ke dua PC1 Melakukan panggilan pada HP1 selama 1 – 6 menit, kemudian ditahap akhir di cari nilai rata-rata dari 6 kali percobaan tersebut.

3. *Packet Loss*

Pengujian parameter *Packet loss* dilakukan untuk mengetahui nilai QoS, semakin rendah nilai *Packet loss* yang diperoleh maka dinilai kualitas sangat baik. Begitu juga sebaliknya semakin tinggi nilai *Packet Loss* yang diperoleh maka kualitas sangat buruk. Proses pengujian ini di lakukan dengan 6 kali percobaan panggilan, dengan rentang waktu 1-6 menit. Percobaan pertama Laptop1 melakukan panggilan pada HP1 selama 1-6 menit, percobaan ke dua PC1 melakukan panggilan pada HP1 selama 1 – 6 menit, kemudian ditahap akhir di cari nilai rata-rata dari 6 kali percobaan tersebut.

4. Mekanisme Pengujian Keamanan

Mekanisme pengujian keamanan VPN pada jaringan VoIP dengan serangan MITM pada saat *client* melakukan komunikasi menggunakan dua kondisi, yaitu: pengujian keamanan pangilan kedua *client* terhubung dengan VPN dan pengujian keamanan panggilan salah satu *client* yang terhubung dengan VPN, berikut mekanismenya:

a) Pengujian Panggilan kedua *client* terhubung dengan VPN

Pengujian ini di lakukan dengan cara client saling komunikasi dengan rentang waktu 2-4 menit, yaitu Laptop 1 menghubungi HP1, kemudian komputer *Attacker* melakukan *sniffing* atau melakukan serangan terhadap *client* yang sedang komunikasi. Serangan tersebut ingin mengetahui tingkat keamanan VPN pada jaringan VoIP, apakah *Attacker* dapat mendengarkan percakapan antara *client* tersebut apa tidak, serangan MITM ini menggunakan *software Cain and abel.*

b) Pengujian Panggilan salah satu *client* terhubung dengan VPN

Pengujian ke dua ini tidak jauh beda dengan pengujian pertama, perbedaan hanya pada client yang melakukan komunikasi, yaitu PC1 menghubungi HP1 dengan rentang waktu 2-4 menit. Kemudian komputer *Attacker* melakukan *sniffing* atau melakukan serangan terhadap *client* yang sedang komunikasi, serangan tersebut ingin mengetahui tingkat keamanan VPN pada jaringan VoIP, apakah *Attacker* dapat mendengarkan percakapan antara *client* tersebut atau tidak, serangan MITM ini menggunakan *software Cain and abel.*

PEMBAHASAN

Pengujian kualitas menggunakan tiga pengukuran *QOS (Quality of Service),* sedangkan keamanannya di uji dengan menggunakan serangan MITM. Aplikasi pendukung yang digunakan yaitu aplikasi *Wireshark* dan *cain and abel,* hasil pengujian sebagai berikut:

a. Mencari Nilai QoS pada Jaringan VoIP

Pengujian analisis VoIP ini menggunakan tiga pengukuran *Quality of service (QoS)* yaitu, *Delay, Throughput* dan *Packet loss,* aplikasi yang digunakan unutk mencari nilai QoS tersebut adalah *Wireshark.* Berikut ini langkah-langkah mencari nilai QoS:

1. Menjalankan sistem VoIP Server yang sudah di-*setting* pada PC Server
2. Menjalankan aplikasi *Wireshark*
3. Client melakukan komunikasi sesuai dengan rencana pengujian.

Pada aplikasi *Wireshark* akan terlihat protokol yang sedang bekerja selama proses komunikasi berlangsung, dan untuk mendapatkan nilai *Delay, Throughput, packet loss,* proses capture pada aplikasi *Wireshark* harus di stop terlebih dahulu, berikut hasil *capture* dan perhitungan masing-masing parameter QoS dengan menggunakan aplikasi *Wireshark*:

Statistics

Measurement	Captured	Displayed	Marked
Packets	9338	9338 (100.0%)	—
Time span, s	70.453	70.453	—
Average pps	132.5	132.5	—
Average packet size, B	203	203	—
Bytes	1893750	1893750 (100.0%)	0
Average bytes/s	26k	26k	—
Average bits/s	215k	215k	—

Gambar 4**.** Hasil Capture Wireshark

1. *Delay*

Pada gambar 4 berikut menunjukkan data hasil capture wireshark, dan berdasarkan data yang diperoleh dari *Wireshark,* maka diperoleh nilai *delay* dengan cara perhitungan sebagai berikut:

Delay = Total Delay / Paket yang dikirim

= 70,453 / 9338 s

= 0,0075 s

= 7.5447 ms

2. *Throughput*

Berdasarkan data yang diperoleh dari *Wireshark,* maka diperoleh nilai *throughput* dengan cara perhitungan sebagai berikut:

Throughput = Jumlah data yang dikirim / Waktu pengiriman data

= *1893750/70,453*

= *26,879 x 8*

= *215 bps*

3. *Packet Loss*

Berdasarkan data yang diperoleh dari *Wireshark,* maka diperoleh nilai *Packet loss* dengan cara perhitungan sebagai berikut:

Packet loss = Paket yang dikirim – paket yang ditrima x 100 % / Paket yang dikirim

= 9338-9338 x 100% / 9338

= 0,0 %

b. Analisis Nilai QoS pada jaringan VoIP

Analisis nilai QoS pada jaringan VoIP dengan 6 kali pengujian rentang waktu 1 – 6 menit pada pangilan Laptop1 ke HP1 dan PC1 ke HP1, yaitu *Delay*, *Throughput dan Packet loss*, berikut analisisnya:

1. *Delay*

Tabel 2 Nilai *Delay* pada panggilan Laptop 1 ke HP1

Percobaan	Waktu	Status	*Delay* (ms)	Keterangan
Percobaan 1	Panggilan selama 1 Menit	Laptop1 menghubungi HP1	8,059 ms	Baik
Percobaan 2	Panggilan selama 2 Menit		7,511 ms	Baik
Percobaan 3	Panggilan selama 3 Menit		7,515 ms	Baik
Percobaan 4	Panggilan selama 4 Menit		10,679 ms	Baik
Percobaan 5	Panggilan selama 5 Menit		7,085 ms	Baik
Percobaan 6	Panggilan selama 6 Menit		5,699 ms	Baik
Rata-rata			7,758 ms	Baik

[Sumber : Hasil Perhitungan]

Analisis data dari tabel diatas adalah dapat dilihat nilai *Delay* pada panggilan Laptop1 ke HP1 percobaan ke 1 selama 1 menit diperoleh nilai 8,059 ms, percobaan ke 2 selama 2 menit diperoleh nilai 7,511 ms, percobaan ke 3 selama 3 menit diperoleh nilai 7,515 ms, percobaan ke 4 selama 4 menit diperoleh nilai 10,679 ms, percobaan ke 5 selama 5 menit diperoleh nilai 7,085 ms, percobaan ke 6 selama 6 menit diperoleh nilai 5,699 ms. Berdasarkan hasil pengujian selama rentang waktu 1-6 menit diperoleh nilai rata-rata 7,758 ms dan dinilai kualitas baik.

Tabel 3 Nilai *Delay* pada Panggilan PC1 ke HP1

Percobaan	Waktu	Status	*Delay* (ms)	Keterangan
Percobaan 1	Panggilan selama 1 Menit	PC1 menghubungi HP1	7,545 ms	Baik
Percobaan 2	Panggilan selama 2 Menit		7,816 ms	Baik
Percobaan 3	Panggilan selama 3 Menit		7,632 ms	Baik
Percobaan 4	Panggilan selama 4 Menit		7,600 ms	Baik
Percobaan 5	Panggilan selama 5 Menit		7,562 ms	Baik
Percobaan 6	Panggilan selama 6 Menit		7,787 ms	Baik
Rata-rata			7,657 ms	Baik

[Sumber : Hasil Perhitungan]

Analisis data dari tabel diatas adalah dapat dilihat nilai *delay* pada panggilan PC1 ke HP1 percobaan ke 1 selama 1 menit diperoleh nilai 7,545 ms, percobaan ke 2 selama 2 menit diperoleh nilai 7,816 ms, percobaan ke 3 selama 3 menit diperoleh nilai 7,636 ms, percobaan ke 4 selama 4 menit diperoleh nilai 7,600 ms, percobaan ke 5 selama 5 menit diperoleh nilai 7,562 ms, percobaan ke 6 selama 6 menit

diperoleh nilai 7,787 ms. Berdasarkan hasil pengujian selama rentang waktu 1-6 menit diperoleh nilai rata-rata 7,657 ms dan dinilai kualitas baik.

2. *Throughput*

Tabel 4 Nilai *Throughput* Pada panggilan Laptop1 ke HP1

Percobaan	Waktu	Status	*Throughput*(bps)
Percobaan 1	Panggilan selama 1 Menit	Laptop1 menghubungi HP1	239 bps
Percobaan 2	Panggilan selama 2 Menit		258 bps
Percobaan 3	Panggilan selama 3 Menit		256 bps
Percobaan 4	Panggilan selama 4 Menit		178 bps
Percobaan 5	Panggilan selama 5 Menit		297 bps
Percobaan 6	Panggilan selama 6 Menit		566 bps
Rata-rata			299 bps

[Sumber : Hasil Perhitungan]

Analisis data dari tabel diatas adalah dapat dilihat nilai *Throughput* pada panggilan Laptop1 ke HP1 percobaan ke 1 selama 1 menit diperoleh nilai 239 bps, percobaan ke 2 selama 2 menit diperoleh nilai 258 bps, percobaan ke 3 selama 3 menit diperoleh nilai 256 bps, percobaan ke 4 selama 4 menit diperoleh nilai 178 bps, percobaan ke 5 selama 5 menit diperoleh nilai 297 bps, percobaan ke 6 selama 6 menit diperoleh nilai 566 bps. Berdasarkan hasil pengujian selama rentang waktu 1-6 menit diperoleh nilai rata-rata 299 bps.

Tabel 5 Nilai *Throughput* Pada Panggilan PC1 ke HP1

Percobaan	Waktu	Status	*Throughput*(bps)
Percobaan 1	Panggilan selama 1 Menit	PC1 menghubungi HP1	215 bps
Percobaan 2	Panggilan selama 2 Menit		206 bps
Percobaan 3	Panggilan selama 3 Menit		210 bps
Percobaan 4	Panggilan selama 4 Menit		212 bps
Percobaan 5	Panggilan selama 5 Menit		212 bps
Percobaan 6	Panggilan selama 6 Menit		206 bps
Rata-rata			210 bps

Analisis data dari tabel diatas adalah dapat dilihat nilai *Throughput* pada panggilan PC1 ke HP1 percobaan ke 1 selama 1 menit diperoleh nilai 215 bps, percobaan ke 2 selama 2 menit diperoleh nilai 206 bps, percobaan ke 3 selama 3 menit diperoleh nilai 210 bps, percobaan ke 4 selama 4 menit diperoleh nilai 212 bps, percobaan ke 5 selama 5 menit diperoleh nilai 212 bps, percobaan ke 6 selama 6 menit diperoleh nilai 206 bps. Berdasarkan hasil pengujian selama rentang waktu 1-6 menit diperoleh nilai rata-rata 210 bps.

3. *Packet Loss*

Tabel 6 Nilai *Packet loss* Pada Panggilan Laptop1 ke HP1

Percobaan	Waktu	Status	*Packet loss* (%)	Keterangan
Percobaan 1	Panggilan selama 1 Menit	Laptop1 menghubungi HP1	0 %	Sangat Baik
Percobaan 2	Panggilan selama 2 Menit		0 %	Sangat Baik
Percobaan 3	Panggilan selama 3 Menit		0 %	Sangat Baik
Percobaan 4	Panggilan selama 4 Menit		0 %	Sangat Baik
Percobaan 5	Panggilan selama 5 Menit		0 %	Sangat Baik
Percobaan 6	Panggilan selama 6 Menit		0 %	Sangat Baik
Rata-rata			0 %	Sangat Baik

[Sumber : Hasil Perhitungan]

Analisis data dari tabel diatas adalah dapat dilihat nilai *Packet loss* pada panggilan Laptop1 ke HP1 percobaan ke 1 selama 1 menit didapat nilai 0%, percobaan ke 2 selama 2 menit didapat nilai 0%, percobaan ke 3 selama 3 menit didapat nilai 0%, percobaan ke 4 selama 4 menit didapat nilai 0%, percobaan ke 5 selama 5 menit didapat nilai 0%, percobaan ke 6 selama 6 menit didapat nilai 0%. Berdasarkan hasil pengujian selama rentang waktu 1-6 menit diperoleh nilai rata-rata 0%, dan dinilai kualitas sangat baik.

Tabel 7 Nilai *Packet loss* Pada panggilan PC1 ke HP1

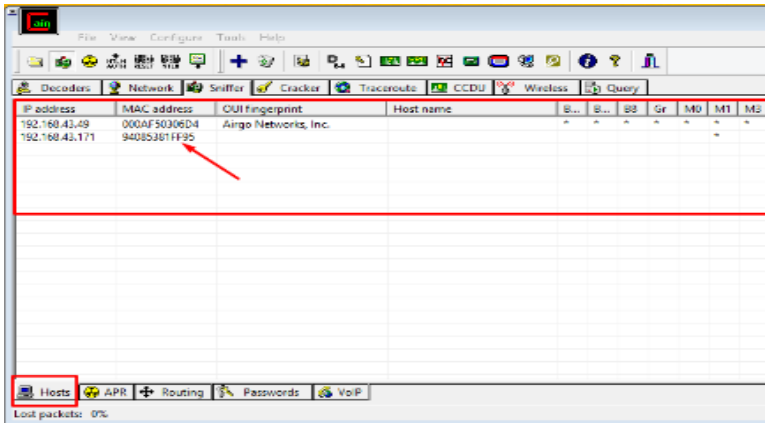
Percobaan	Waktu	Status	*Packet loss* (%)	Keterangan
Percobaan 1	Panggilan selama 1 Menit	PC1 menghubungi HP1	0 %	Sangat Baik
Percobaan 2	Panggilan selama 2 Menit		0 %	Sangat Baik
Percobaan 3	Panggilan selama 3 Menit		0 %	Sangat Baik
Percobaan 4	Panggilan selama 4 Menit		0 %	Sangat Baik
Percobaan 5	Panggilan selama 5 Menit		0 %	Sangat Baik
Percobaan 6	Panggilan selama 6 Menit		0 %	Sangat Baik
Rata-rata			0 %	Sangat Baik

Analisis data dari tabel diatas adalah dapat dilihat nilai *Packet loss* pada panggilan PC1 ke HP1 percobaan ke 1 selama 1 menit diperoleh nilai 0%, percobaan ke 2 selama 2 menit diperoleh nilai 0%, percobaan ke 3 selama 3 menit diperoleh nilai 0%, percobaan ke 4 selama 4 menit diperoleh nilai 0%, percobaan ke 5 selama 5 menit diperoleh nilai 0%, percobaan ke 6 selama 6 menit diperoleh nilai 0%. Berdasarkan hasil pengujian selama rentang waktu 1-6 menit diperoleh nilai rata-rata 0%, dan dinilai kualitas sangat baik.

4. Analisis *Keamanan* VOIP

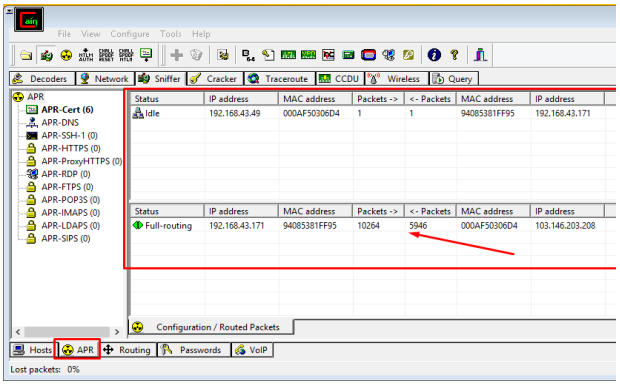
Analisis keamanan VoIP ini dilakukan dengan dua cara pengujian agar diperoleh perbedaan kualitas keamanan VPN dari serangan MITM, yaitu kedua *client* terhubung dengan VPN dan salah satu client terhubung dengan VPN, kemudian diuji keamanan dengan melakukan serangan MITM menggunakan *software cain and abel*. Skema pengujiannya *client* 1 menghubungi *client* 2 dan *attacker* berada di tengah-tengah antara *client* 1 dan *client* 2. Adapun analisis keamanannya menggunakan *software cain and abel* sebagai berikut:

a) Pengujian Panggilan Kedua Client Terhubung Dengan VPN



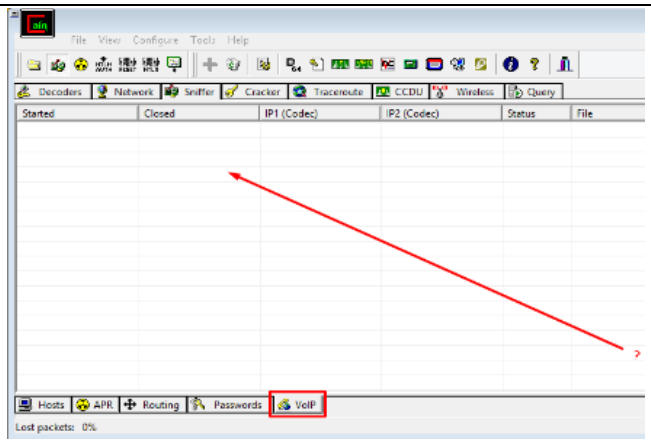
Gambar 5. Proses *Scanning Mac address client* Laptop1 ke HP1
[Sumber : Tangkap layar hasil penelitian]

Pada gambar diatas menunjukkan bahwa *attacker* dapat melakukan *scanning* terhadap *client* yang sedang melakukan komunikasi, ditunjukkan dengan *attacker* dapat melihat IP dan *MAC address client* tersebut.



Gambar 6 Proses *Arpspoofing* Laptop1 ke HP1
[Sumber : Tangkap layar hasil penelitian]

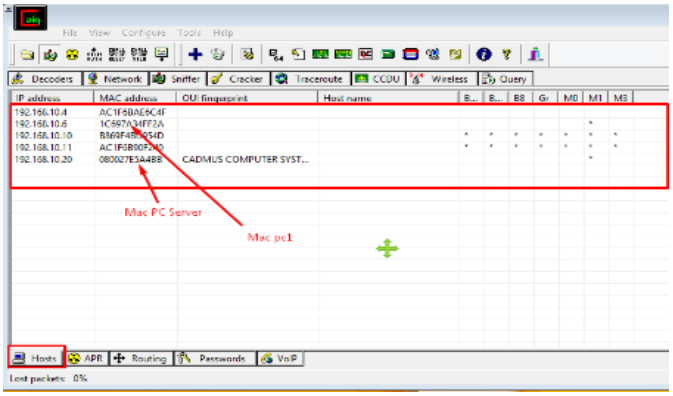
Pada gambar diatas menunjukkan bahwa *attacker* berhasil melakukan *Arpspoofing* terhadap *client* yang sedang melakukan komunikasi. Pada tahap ini *attacker* akan bertindak sebagai MITM. Namun pada pengujian dengan menggunakan VPN *Attacker hanya dapat* melihat jumlah packet data yang dikirim, tidak dapat melakukan serangan dengan mengirimkan *mac address* miliknya kepada salah satu *client* yang berkomunikasi.



Gambar 7. VoIP *Recording* Laptop1 ke HP1
[Sumber : Tangkap layar hasil penelitian]

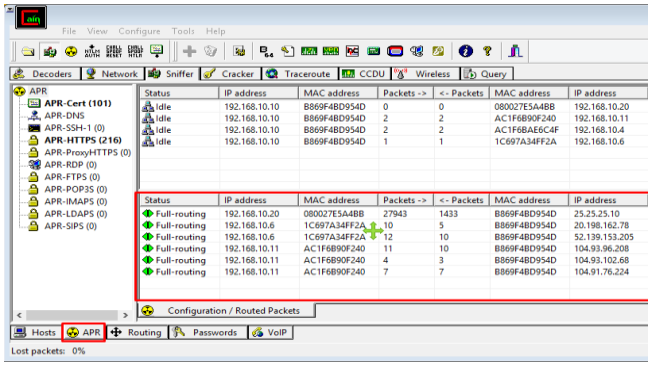
Pada gambar diatas menunjukkan bahwa *attacker* tidak dapat merekam atau mendengarkan percakapan *client* yang sedang melakukan komunikasi.

b) Pengujian Panggilan Salah Satu Client Terhubung Dengan VPN



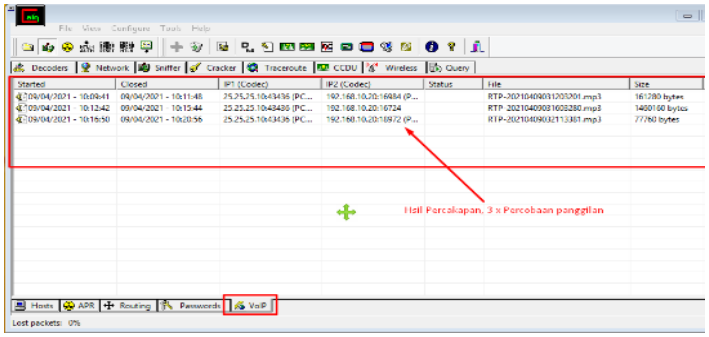
Gambar 8. Proses *Scanning Mac address client* PC1 ke HP1
[Sumber : Tangkap layar hasil penelitian]

Pengujian keamanan hanya menggunakan satu *client* saja yang terhubung dengan VPN dan *client* satunya tidak terhubung dengan VPN. Pada proses *scanning mac address attacker* dapat melihat IP dan *Mac address* lebih banyak daripada proses yang pertama. Karena *Software Cain and abel* dapat membaca perangkat-perangkat lokal yang saling terhubung, salah satunya IP dan *Mac address* komputer *server* dapat terbaca juga.



Gambar 8. Proses *Arpspoofing* PC1 ke HP1
[Sumber : Tangkap layar hasil penelitian]

Pada gambar diatas menunjukkan bahwa *attacker* berhasil melakukan *Arpspoofing* terhadap *client* yang sedang melakukan komunikasi, pada tahap ini *attacker* akan bertindak sebagai MITM yang akan mengirimkan *mac address* miliknya kepada salah satu *client* yang berkomunikasi dan akan menyebabkan *client* tersebut dibanjiri *spoofing mac address. Client* pun akan beranggapan bahwa *mac address* dari *attacker* tersebut sah. Hal ini membuktikan bahwa sistem VoIP standar tidak memiliki perlindungan terhadap aspek kerahasiaan dan kepercayaan data dari serangan *Main in The Middle* (MITM).



Gambar 9. VoIP *Recording* PC1 ke HP1 [Sumber : Tangkap layar hasil penelitian]

Pada gambar diatas percobaan panggilan 3 kali *Attacker* dapat merekam dan mendengarkan percakapan *client* yang melakukan komunikasi, namun hasil rekaman yang di dapat tidak sama dengan waktu panggilan *client* tersebut yang berarti hasil rekaman yang diperoleh tidak utuh 100%. Hal tersebut menunjukkan bahwa *attacker* berhasil mendapatkan percakapan *client* yang sedang melakukan komunikasi.

KESIMPULAN

Berdasarkan hasil dan pembahasan yang sudah dipaparkan, maka diperoleh kesimpulan sebagai berikut:

a. Nilai QoS dengan 6 kali pengujian rentang waktu 1-6 menit diperoleh nilai rata-rata *Delay* 7,758 ms 7,657 ms, dan 299 bps, 210 bps, serta *Packet loss* 0%.
b. Analisis keamanan VoIP dengan menggunakan dua skenario pengujian, skenario pertama diperoleh data VoIP antara dua *client* yang sama-sama terhubung dengan VPN, *attacker* hanya

dapat melakukan *scan* IP dan *MAC address* saja, namun tidak dapat merekam atau mendengarkan percakapan antara *client* yang saling berkomunikasi. Pada skenario kedua, salah satu *client* terhubung dengan VPN, *attacker* dapat melakukan *scan* IP dan *MAC Address*, namun tidak hanya dua perangkat itu yang mampu di-*scan* IP dan *MAC address*-nya, tetapi *attacker* juga dapat merekam dan mendengarkan percakapan antara dua *client* tersebut, namun percakapan yang terekam hanya singkat.

REFERENSI

Abdoe R.S., (2017), *Analisis Kinerja VoIP Open Source FreePBX Asterisk Menggunakan Metode MOS- E-Model (ITU-T.G.107).*Universitas Muhammadiyah Jember.

Ahmad, F., (2011), *Uji Kemanan Sistem Komunikasi VoIP dengan Pemanfaatan Fasilitas Enkripsi Pada Open VPN*, Universitas Syarif Hidayatullah Jakarta.

Amarudin, DKK (2014). *Analisis keamanan jaringan single sign on (sso) Dengan lightweight directory access protocol (ldap) Menggunakan metode MITMA*.Universitas Gadjah Mada Yogyakarta.

Anjar, S. (2013). *Analisis Simulasi Mobile VoIP (Voice Over Internet Protocol) Berbasis SIP(Session Initiaton Protocol) Pada jaringan Wireless digedung FTI UKSW,* Universitas Kristen Satya Wacana Salatiga.

Ari, P.W. (2017). *Optimasi Jaringan Local Are Network Menggunakan VLAN dan VOIP*, Universitas Widyatama.

Cahyanto, T. A., Oktavianto, H., & Royan, A. W. (2016). Analisis dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan. JUSTINDO (Jurnal Sistem Dan Teknologi Informasi Indonesia), 1(2).

Domiko, F.J.P., dkk., (2012), *Analisa perancangan server voip (voice internet protocol) Dengan opensource asterisk dan vpn (virtual privatenetwork) Sebagai pengaman jaringan antar client,* Universitas Lampung.

Eko, B.S., (2012), *Analisa quality of services (QOS) voice over interneProtocol (VoIP) dengan protokol h.323 dan session Initial protocol (sip),* Program Studi Teknik Informatika UNIKOM Bandung.

Harun Sujadi, Aqis Mutaqin., (2017), *Rancang Bangun Arsitektur Jaringan Komputer Teknologi Metropolitan Area Network (Man) Dengan Menggunakan Metode Network Development Life Cycle (Ndlc).*Universitas Majalengka.

Hari R., Bowo N., (2012), *Analisis implementasi keamanan jaringan virtual Private network (VPN) pada Pt. Layar sentosa shipping corporation*, Universitas Dian Nuswantoro.

Junaedi A.P., dkk., (2017), *Investigasi Performa VoIP Pada jaringan Wireless dengan menggunakan server Elastix*. Politeknik Negeri Banyuwangi.

Laurentinus, (2015), *Rancang bangun server voisce over internet Protocol (VOIP) dengan pengamanan virtual Private network (VPN) studi kasus Stmik Atma Luhur*, Teknik Informatika Stmik Atma Luhur Pangkalpinang.

Winarno, N., & Cahyanto, T. (2021). Penggunaan Karakter Kontrol ASCII Untuk Integrasi Data Pada Hasil Enkripsi Algoritma Caesar Cipher. INFORMAL: Informatics Journal, 6(3), 197-204. doi:10.19184/isj.v6i3.21091.

Yaqin, M. A., Cahyanto, T. A., & Fitriyah, N. Q. (2021). Metode Live Memory Acquisition untuk Pencarian Artefak Digital Perangkat Memori Laptop Berdasarkan Simulasi Kasus Kejahatan Siber. BIOS: Jurnal Teknologi Informasi Dan Rekayasa Komputer, 2(2), 87-94.