ANALISIS PROTOKOL SECURE SOCKET LAYER DENGAN SERANGAN IP SPOOFING, HEARTBLEED BUG, DDOS, MAN-IN-THE-MIDDLE ATTACK: VIDEO HIJACKING, SERTA KOMBINASI SERANGAN

ANALYSIS SECURE SOCKET LAYER PROTOCOL WITH IP SPOOFING, HEARTBLEED BUG, DDOS, MAN-IN-THE-MIDDLE ATTACK: VIDEO HIJACKING, AND ATTACK COMBINATION

Jafar Alim Habibi[1], Rendy Munadi[2], Leanna Vidya Yovita[3]

[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

[1]jafaralimhabibi@students.telkomuniversity.ac.id, [2]rendymunadi@telkomuniversity.ac.id, [3]leanna@telkomuniversity.ac.id

Abstrak

Komunikasi one-way berupa video saat ini semakin mudah digunakan. Salah satu layanan yang mempermudah akses komunikasi tersebut adalah *Internet Protocol Tele Vision* (IPTV). Dengan kemudahan layanan berbasis packet switch yang sudah masuk di seluruh wilayah di dunia semakin mempermudah akses dari layanan IPTV. Regulasi dari IPTV, yang membutuhkan performansi tinggi, membuat layanan ini diminati oleh masyarakat luas. Namun, mudahnya akses dari layanan tersebut membuat tingkat keamanan yang digunakan perlu dianalisis lebih lanjut. Sebagai pengujian keamanan dari layanan IPTV, penelitian ini menggunakan 5 serangan secara bertahap, *yaitu Distributed Denial-of-Service (DDoS), IP Spoofing, Man-in- the-Middle Attack: Video Hijacking, Heartbleed Bug,* serta satu kombinasi dari *IP Spoofing-Distributed Denial- of-Service (DDoS)-Man-in-the-Middle Attack: Video Hijacking,* dengan *hacker* atau *pentest* bukan berasal dari penguji sendiri. Dalam tugas akhir ini, analisis penelitian diambil dari 3 skenario: menggunakan program VLC, menggunakan *web page-interface*, serta menggunakan *web-page-interface* setelah diserang oleh *pentest* atau *hacker*, dengan *routing protocol* berupa *Open-Shortest Path First* (OSPF) dan menggunakan *Protocol Independent Multicast* (PIM) sebagai pengelompokan alamat IP video.

Kata kunci: IPTV, Secure Socket Layer, Performansi Serangan

Abstract

One-way communications such as video streaming nowadays are easier to be used. One of service which eases those communications is Internet Protocol Tele Vision (IPTV). By easiness of service packet-based that has entered in the whole of world made simplifies access of IPTV services. The regulation of IPTV, which needs high performance, makes these services interesting to any people. However, the easier access requires secure services for protecting data and information. This research uses 5 type of attacks simultaneously, those are Distributed Denial-of-Service (DDoS), IP Spoofing, Man-in-the-Middle Attack: Video Hijacking, Heartbleed Bug, and a combination from IP Spoofing-DDoS-MitM Attack: Video Hijacking, with hacker or penetration tester (pentest) does not belong to examiner. In the final task, the experiments of analysis are taken from 3 scenarios: using VLC program, web page-interface, and web page-interface after being attacked by pentest or hacker, with Open-Shortest Path First (OSPF) as routing protocol, and Protocol Independent Multicast (PIM) as grouping of videos IP.

Keywords: IPTV, Secure Socket Layer, Attacks Performances

1. Pendahuluan

IPTV didefinisikan sebagai layanan multimedia seperti televisi, video, audio, teks, grafik maupun data yang terkirimkan berdasarkan jaringan IP yang sudah termanajemen dan sudah terjamin dari faktor QoS, pengalaman, sekuritas, interaktif serta kehandalan [4]. Maka dari itu, faktor sekuritas adalah prioritas utama untuk pelayanan IPTV karena konten video yang diproduksi tidak selalu memberikan hak lisensi untuk mendistribusikan konten berbasis premium melalui jaringan digital, kecuali ada mekanisme yang kuat pada suatu wilayah atau daerah, untuk memberikan keamanan lebih pada konten tersebut [5].

Masalah utamanya adalah ketika penggunaan jaringan tersebut dilakukan berbasis IP, dimana pada jaringan tersebut sangat rentan terjadi serangan atau ancaman dari pihak luar. Menurut William Stalling, serangan terbagi menjadi 2, yaitu *passive attack* dan *active attack*, dimana *passive attack* adalah serangan yang berfungsi untuk membaca atau melihat informasi yang ada, tanpa mempengaruhi sistem keamanan jaringan, sedangkan *active attack* adalah serangan yang memiliki fungsi untuk merusak atau memodifikasi atau menghilangkan informasi yang telah atau akan masuk pada suatu sistem jaringan [8].

Maka dari itu, dibutuhkan penelitian apakah serangan berbasis IP mampu mengancam kualitas dan keamanan dari layanan berbasis IPTV ini. Pada penelitian ini disediakan 5 serangan secara bertahap, yaitu *Distributed Denial-of-Service (DDoS), IP Spoofing, Man-in-the-Middle Attack: Video Hijacking, Heartbleed Bug,* serta satu kombinasi dari *IP Spoofing-Distributed Denial-of-Service (DDoS)-Man-in-the-Middle Attack: Video Hijacking*, dengan *hacker* atau *pentest* bukan berasal dari penguji sendiri.

Distributed Denial of Service (DDoS) adalah salah satu tipe dari *cyberattack* yang paling rumit, dimana mendapat perhatian besar pada jaringan di pemerintahan dan institusi – institusi besar saat ini [2]. Serangan ini bersifat tersembunyi dan membahayakan sistem jaringan *online* pada provider layanan sebagai bisnis mereka (*attacker*) yang tergantung pada ketersediaan web site dari provider jaringan untuk membuat bisnis dari provider jaringan menjadi kritis dan produktivitas menurun drastis [2].

IP Spoofing merupakan penciptaan dari paket IP yang digunakan oleh seseorang untuk mencari sumber alamat IP suatu jaringan [1]. Teknik ini digunakan untuk berbagai alasan dan dikembangkan dalam berbagai serangan [1]. Pada penggunaan teknik serangan IP spoofing sendiri lebih banyak dikombinasikan dengan serangan yang lain, misalnya IP spoofing dikombinasikan dengan DDoS, atau dengan kombinasi yang lain.

Dalam perkembangannya di keamanan jaringan, penggunaan serangan man-in-the middle attack lebih dimodifikasikan dengan cara menggunakan serangan *hijacking* sebagai tujuan akhir serangan tersebut. *Hijacking* merupakan salah satu dari tipe serangan keamanan jaringan dimana *attacker* mengendalikan komunikasi secara utuh antara dua entitas dan menyamarkan satu dengan yang lain [6].

Vulnerability Heartbleed bug bukan termasuk dalam serangan yang diperhitungkan dalam keamanan jaringan. Jenis *vulnerability* ini teridentifikasi secara formal pada CVE-2014-0160 [9]. Jenis ini ditemukan dari hasil *buffer overread* dalam pengimplementasian OpenSSL dalam penambahan TLS heartbeat [10].

2. Perancangan Sistem

2.1. Perancangan Skenario

Dalam penelitian ini dirancang 3 skenario yang tujuan akhirnya adalah sebagai pengambilan data awal dan akhir dari serangan yang ada. Skenario ini bertujuan untuk meneliti dan menganalisis bagaimana kondisi performansi dari layanan IPTV yang diambil sebelum dan sesudah serangan terjadi, agar bisa diambil kesimpulan apakah serangan yang telah ditetapkan sebelumnya merupakan serangan yang berpengaruh besar pada layanan IPTV yang diterapkan atau tidak, sehingga dapat diambil saran untuk kedepannya bagaimana sistem layanan IPTV yang baik jika serangan yang ditetapkan tersebut terjadi.

Pada skema serangan ini, jaringan dibuat dengan sistem jaringan *private* atau dalam hal ini menggunakan jaringan intranet. Dalam pengujian ini, diuji cobakan 5 serangan dari setiap serangan yang bertujuan untuk mengubah, menembus, atau mengganggu dari sistem kerja dari protokol *Secure Socket Layer* dalam jaringan IPTV ini. Dalam percobaan ini juga dianalisis apakah terdapat efek dari penyerangan yang dilakukan oleh *hacker* terhadap pengguna/*client* dari layanan IPTV ini.

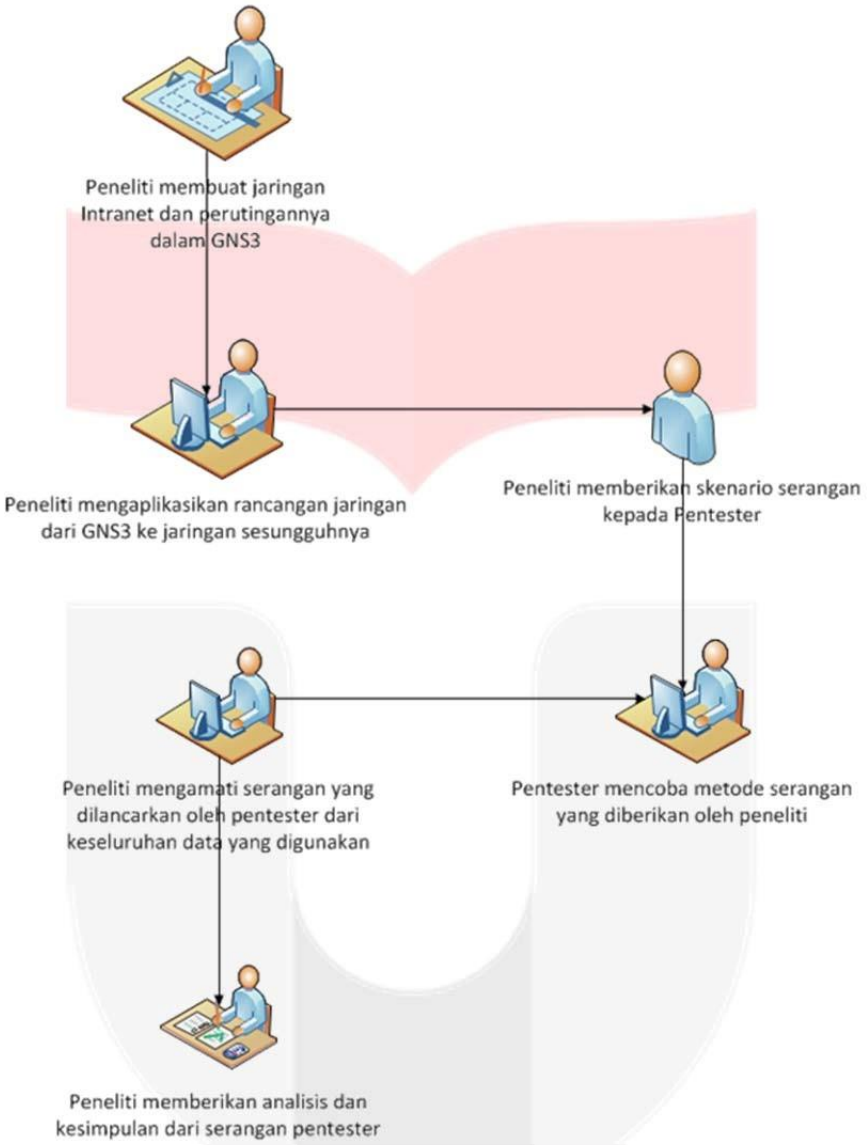
Berikut adalah skema serangan dari penilitian ini:

1. Semua pengguna layanan jaringan IPTV harus melakukan *login session*, dimana dalam database dari *client* dan *server* terenkripsi dengan metode algoritma *hash function* MD5.
2. Client dan server sudah didaftarkan sebelumnya, dan client atau pengguna lain (kecuali server) tidak memiliki akses untuk mendaftarkan diri dengan akun lain.
3. Dalam database hanya terdiri dari 10 akun yang sudah dibuat sebelumnya.
4. Attacker sudah memiliki IP sendiri. Namun, dalam skenario ini, attacker atau pentester tidak memiliki akses untuk membuat akun atau mengganti akun yang telah ada.
5. Pengujian dari segi *Quality of Service* (QoS) terdiri dari pengujian menggunakan sistem implementasi dari semua alat yang telah disiapkan (Router, Switch, PC *Client-Server* dan PC *Attacker/Pentester*). Pengujian paket data yang dilihat adalah dari segi UDP dan TCP.
6. Tools yang digunakan untuk melakukan pelacakan dan pengawasan terhadap hasil serangan yang terjadi terdiri dari 2 cara, yaitu dengan menggunakan program seperti Wireshark, dan cara kedua dengan melakukan pengawasan secara manual dari database yang ada dalam jaringan IPTV dan pengkodean dari website yang digunakan.

7. Setiap serangan diuji dengan skema yang sudah dijelaskan sebelumnya. Analisis diambil dalam setiap tahapan yang ada, beserta solusi yang termasuk didalamnya.
8. Peneliti mengambil kesimpulan dan saran dari penelitian yang sudah dilakukan.

Untuk lebih jelasnya, Gambar 1 merupakan dasar skema yang telah dirancang:

Gambar 1 – Dasar skema serangan



2.2. Parameter Pengambilan Data

Pengambilan data menggunakan perangkat lunak dari *Wireshark*, dimana video yang dikirimkan menggunakan aplikasi *VLC*, dengan penerapan *web server* menggunakan Apache dan PhpMyAdmin, dengan seluruh sistem operasi menggunakan Ubuntu 12.04 dan 14.04. Pada Tabel 1 menjelaskan rincian dari metode pengambilan data dari penelitian ini.

Tabel 1 - Daftar Metode Pengambilan Data

No.	Tipe Percobaan	Durasi Pengambilan Data	Konten Video yang diujicobakan	Banyak Percobaan	Parameter yang digunakan	Penggunaan

1.	Hanya menggunakan VLC (Video Server)	30 detik	- Kompas TV playlist - The Imitation Game film - Sherlock 1 Episode 1	10x (untuk RTP)	End-to-end Delay, Throughput, Jitter, Packet Loss	Implementasi
2.	Menggunakan sistem Website (Dengan SSL)	30 detik	- Kompas TV playlist - The Imitation Game film - Sherlock 1 Episode 1	10x (untuk RTP) 5x (untuk HTTPS dan *tracking)*	End-to-end Delay, Throughput, Jitter, Packet Loss	Implementasi
3.	Menggunakan sistem Website + pengujian serangan (Dengan SSL)	30 detik	- Kompas TV playlist - The Imitation Game film - Sherlock 1 Episode 1 (hanya 1 video yang diuji setiap percobaannya)	10x (untuk RTP) 5x (untuk HTTPS dan *tracking)*	End-to-end Delay, Throughput, Jitter, Packet Loss, Round-Trip Time, Source Authentication, Data Integrity, Nonrepudiation	Implementasi

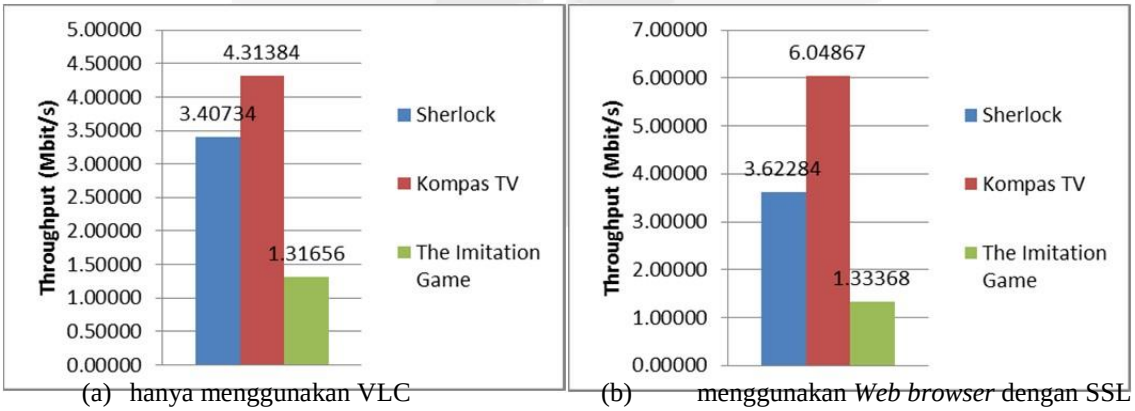
3. Pembahasan

Seperti yang sudah dijelaskan sebelumnya, bahwa penelitian ini bertujuan untuk menganalisis bagaimana serangan yang dilancarkan oleh hacker berhasil atau tidak, maka pada bagian ini perlu adanya penetapan dari segi Quality of Service (QoS) dan keamanan jaringan seperti *Source Authentication,Data Integrity,Nonrepudiation*, kriteria seperti apa sehingga jaringan yang diserang oleh hacker adalah jaringan yang masuk dalam keadaan diserang.

3.1. Parameter *Throughput* dan *Packet Loss*

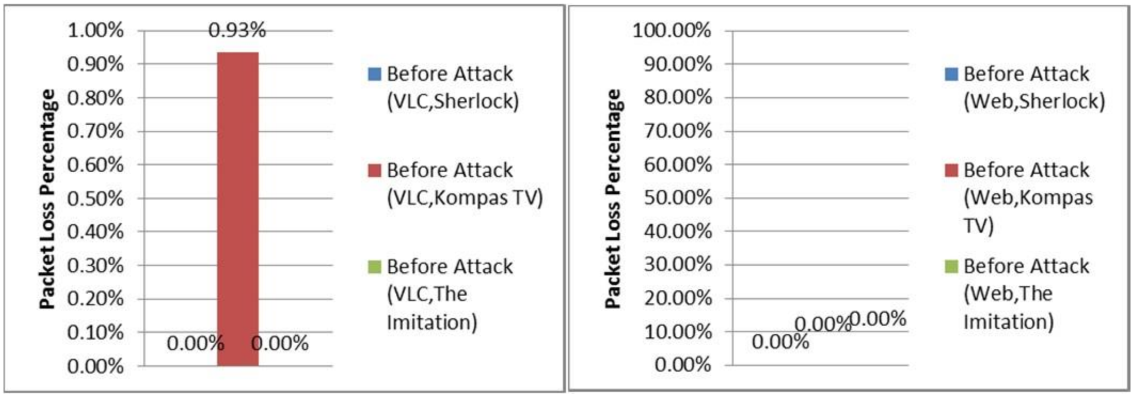
Secara definisi, *throughput* adalah laju rata – rata data yang berhasil diterima oleh penerima [3]. Pada dasarnya, throughput merupakan parameter yang digunakan sebagai landasan dari seberapa cepat data yang dapat diterima oleh penerima dari pengirim, dengan satuan yang digunakan adalah data per waktu.

Secara pengambilan definisi, packet loss merupakan salah satu parameter dalam pengambilan nilai Quality of Service (QoS) yang terjadi karena banyak faktor yang ada, tergantung dari jenis message yang akan dikirimkan.



(a) hanya menggunakan VLC (b) menggunakan *Web browser* dengan SSL

Gambar 2 - Nilai *Throughput* sebelum diserang



(a) hanya menggunakan VLC (b) menggunakan *Web browser* dengan SSL

Gambar 3 – Nilai *Packet Loss* sebelum diserang

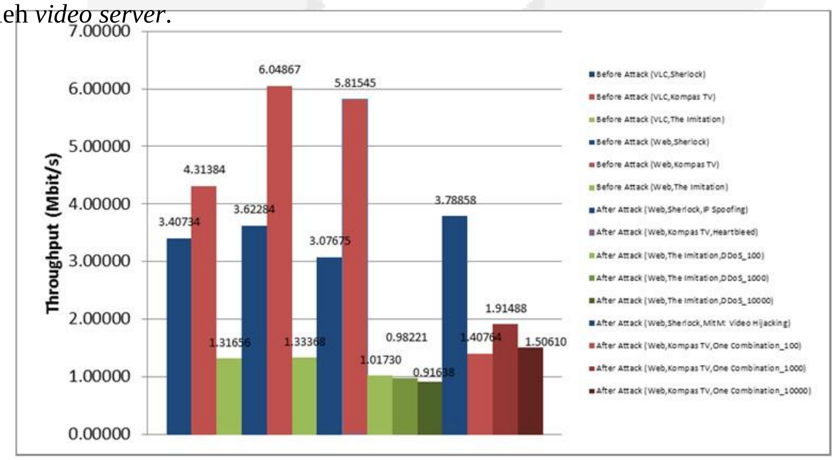
Data dari semua sampel yang diuji menunjukkan nilai throughput rata – rata dari setiap konten yang dijadikan sampel penelitian ini sebesar 3.40734 Mbit/s, 4.31384 Mbit/s, dan 1.31656 Mbit/s. Sedangkan persentase nilai dari packet loss untuk video 1 (Sherlock SE1 EP1) dan video 3 (The Imitation Game) sebesar 0.00%, untuk video 2 (Kompas TV) sebesar 0.93%. Jika menyinggung pada nilai *throughput* yang tidak stabil dari skenario ini bisa dipahami dari total paket yang ter-*capture* dan berjalan pada jaringan tersebut. Berdasarkan formula untuk perhitungan *throughput* sendiri sesuai dengan Persamaan 1, bahwa pengaruh nilai *throughput* bisa dilihat dari banyaknya paket per detik yang diterima oleh pengguna layanan IPTV ini dan besar dari panjang paket dalam setiap paketnya atau lebih sering disebut *packet size*.

[illegible]

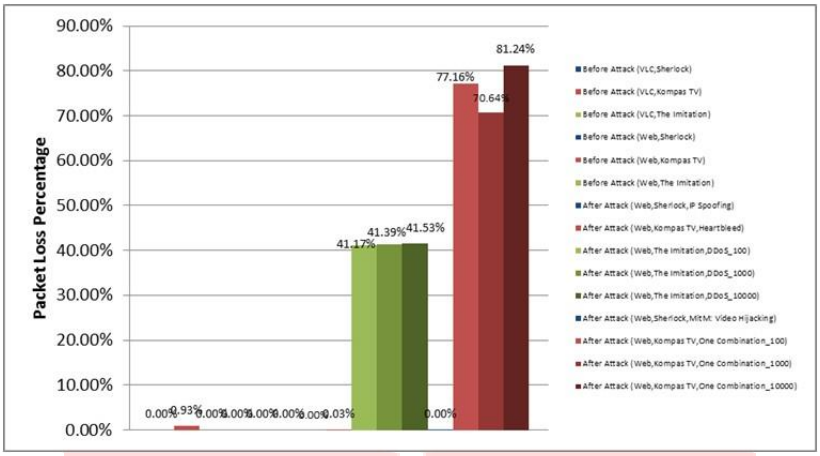
(1)

Persamaan 1. Formula *throughput* dilihat dari *packet size*

Sedangkan nilai *throughput* dan *packet loss* dari jaringan IPTV setelah diserang ditampilkan pada Gambar 4 dan 5. Pada grafik tersebut terlihat bahwa serangan yang berhasil dalam serangan yang dilancarkan terdapat pada serangan DDoS dan kombinasi serangan yang didalamnya terdapat serangan DDoS sebagai salah satu serangan kombinasi. DDoS dapat mengganggu nilai dari *throughput*, dikarenakan paket yang dikirimkan oleh server tidak dapat diterima seluruhnya oleh *client*, sehingga perhitungan paket yang diterima per detik semakin sedikir, sehingga kondisi tersebut dapat menurunkan kualitas dari jaringan sendiri. Sedangkan pada *packet loss*, nilai yang didapat melonjak tajam, dikarenakan *flooding* dari paket lain, sehingga paket yang sebenarnya dikirimkan oleh *server* tidak dapat diterima oleh *client*, maka pilihan utamanya adalah paket didrop secara massal, termasuk paket berupa UDP yang dikirimkan oleh *video server*.



Gambar 4 – Nilai *throughput* setelah diserang

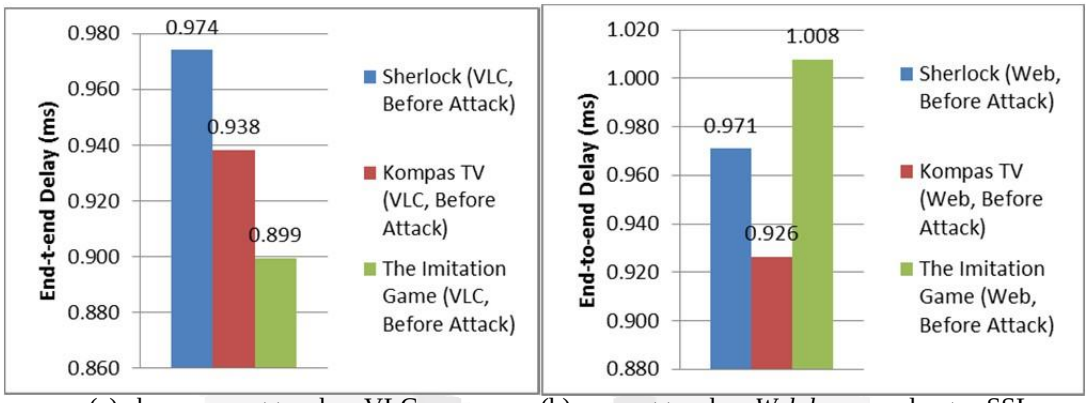


Gambar 5 – Nilai *packet loss* setelah diserang

3.2. Parameter *End-to-end Delay* dan *Jitter*

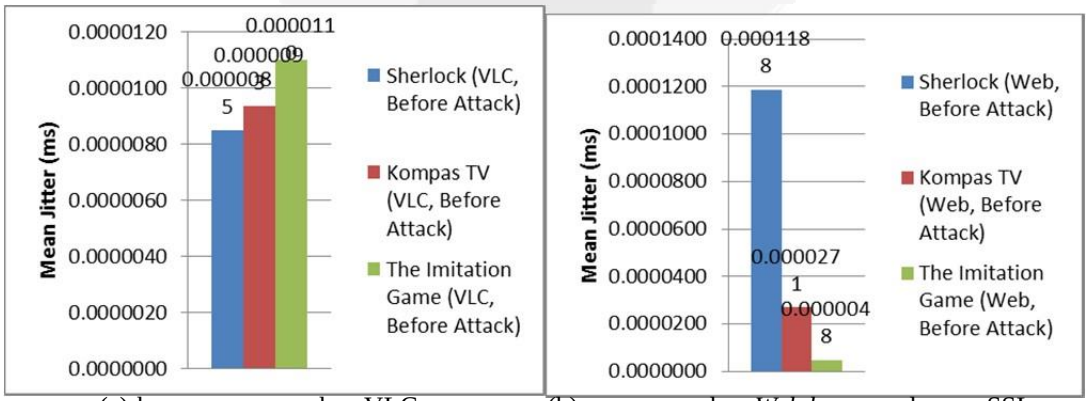
Menurut Kurose Ross, dalam bukunya berjudul Computer Networking: A Top Down Approach, end-to-end delay didefinisikan sebagai akumulasi dari delay pentransmisian, pemrosesan, dan antrian dalam router, delay propagasi dalam jaringan, serta delay pemrosesan dari ujung ke ujung suatu sistem [3].

Jitter merupakan suatu parameter dari suatu jaringan yang terjadi akibat variasi delay dari suatu paket yang dikirimkan dari pengirim ke penerima, sehingga menyebabkan waktu yang terjadi saat delay berbeda – beda dan bersifat fluktuatif [4].



(a) hanya menggunakan VLC (b) menggunakan *Web browser* dengan SSL

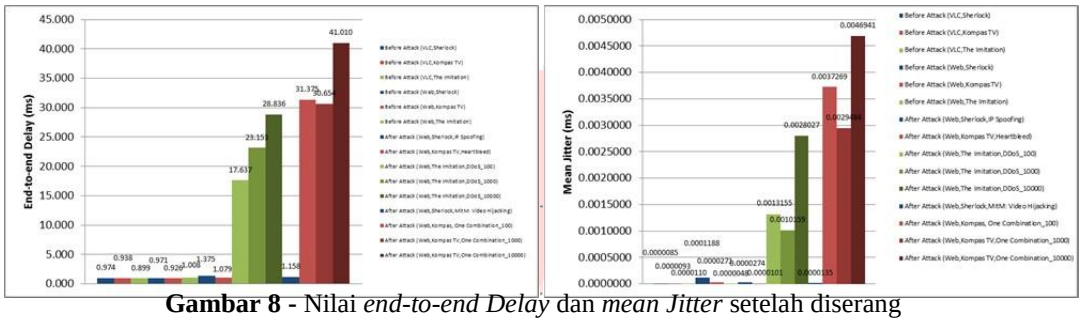
Gambar 6 – Nilai *End-to-end Delay* sebelum diserang



(a) hanya menggunakan VLC (b) menggunakan *Web browser* dengan SSL

Gambar 7 – Nilai *Jitter* sebelum diserang

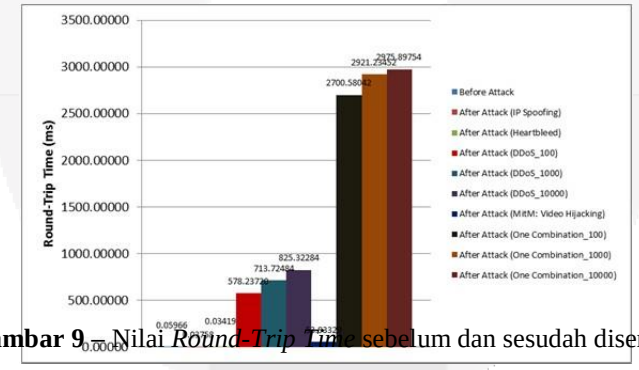
Dari semua sampel yang diuji pada percobaan dengan menggunakan VLC menunjukkan nilai mean jitter dari rata – rata keseluruhan data sebesar 0.0085 µs, 0.0093 µs, 0.0110 µs, serta nilai rata – rata end-to-end delay bernilai 0.974 ms, 0.938 ms, dan 0.899 ms. Perbedaan terjadi pada nilai *end-to-end delay* dari penggunaan IPTV dengan hanya menggunakan VLC dan dengan menggunakan *web page-interface*. Walaupun penurunan yang ditunjukkan tidak mengalami perubahan yang sangat besar, namun penurunan dari nilai *end-to-end delay* pada penggunaan IPTV dengan menggunakan *web page-interface* dinilai sangat bagus. Penurunan dari nilai *end-to-end delay* sendiri bisa menjadi patokan awal bahwa walaupun secara penggunaan *web page* sudah dilindungi oleh HTTPS sebagai protokol aplikasi untuk pengamanan jaringan antara *server* dan *client*, namun tidak mengurangi kualitas dari layanan itu sendiri. Sedangkan nilai *mean jitter* dan *end-to-end delay* setelah diserang dapat dilihat pada Gambar 8. Dari hasil tersebut, dapat dipastikan bahwa serangan yang terjadi dan berhasil menembus keamanan jaringan yang dibentuk terdapat pada serangan DDoS. Ini terjadi karena nilai dari *mean jitter* dan *end-to-end delay* yang naik secara drastis.



Gambar 8 - Nilai *end-to-end Delay* dan *mean Jitter* setelah diserang

3.3. Parameter *Round-Time Trip*

Round-Trip Time (RTT) atau bisa disebut juga round-trip delay adalah waktu yang dibutuhkan bagi sinyal atau paket untuk pengiriman dari sumber khusus ke destinasi yang khusus dan kembali lagi [7]. Secara perhitungannya, RTT adalah perbedaan antara waktu suatu paket yang dikirimkan dengan waktu ACK untuk sebagian paket tersebut diterima [7]. Perhitungan RTT hanya bisa didapatkan pada protokol yang bersifat *connection-oriented* seperti TCP, sehingga pada penelitian ini RTT hanya bisa didapatkan pada koneksi dari *web server* menuju *client.*



Gambar 9 – Nilai *Round-Trip Time* sebelum dan sesudah diserang

4. Kesimpulan

Berdasarkan nilai performansi serangan saat serangan mengalami kegagalan atau keberhasilan dalam melancarkan serangan ke jaringan IPTV yang dibuat, dampak terbesar yang dapat dilihat dalam perhitungan Quality of Service (QoS) adalah terjadi saat serangan Distributed Denial-of-Service (DDoS) dan kombinasi serangan yang melibatkan DDoS sebagai salah satu serangan yang dilancarkan, dengan persentase Packet Loss sebesar 11.37% untuk serangan DDoS dan 58.48% untuk serangan kombinasi yang melibatkan DDoS sebagai salah satu serangan utama. Sedangkan pada serangan yang dilancarkan oleh pentest selain DDoS, tidak terlihat dampak pada perhitungan QoS. Ini disebabkan karena serangan yang terjadi selain DDoS tidak termasuk dalam serangan yang bertipe melancarkan serangan pada jaringan yang dibuat, atau serangan tersebut tidak dapat dideteksi hanya menggunakan perhitungan QoS. Sehingga, terbukti bahwa serangan DDoS lebih tertuju pada bagaimana keamanan pada konfigurasi jaringan yang diserang tersebut dibuat.

Daftar Pustaka

[1] Hofer, C., & Wampfler, R. 2004. *IP SPOOFING*.

[2] Kumar, A. (n.d.). 2013. *DDoS Attacks-A Cyberthreat*. ISACA, 1-4.

[3] Kurose, James F. 2013. *Computer Networking: A Top-Down Approach*. New York: Pearson Inc.

[4] ITU, T. S. 2006, June 13. *Network performance objectives for IP-based services. Y.1541 Series Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS*, 8.

[5] O'Driscoll, G. 2007. *Next Generation IPTV Services and Technologies*. New Jersey: John Wiley & Sons, Inc.

[6] Rouse, M. 2007. TechTarget. *Definition Hijacking.* [Online] Available at: http://searchsecurity.techtarget.com/definition/hijacking. [Accessed 25 October 2014]

[7] Rouse, M. 2007. TechTarget. *Definition Round-Trip Time.* [Online] Available at: http://searchnetworking.techtarget.com/definition/round-trip-time [Accessed 6 October 2015]

[8] Stallings, W. 2006. *Cryptography and Network Security : Principle and Practice (5th ed.).* (M. Horton, T. Dunkelberger, & R. Kernan, Eds.) New York: Pearson Education, Inc.

[9] US-CERT. 2014. [Online] Available at: https://www.us-cert.gov/ncas/alerts/TA14-098A [Accessed 15 April 2015]

[10] Wheeler, D. A. 2014. *Preventing Heartbleed.* IEEE Computer Society, 80-83.