ANALISIS PERBANDINGAN DAMPAK SERANGAN DENIAL OF SERVICE (DOS) TERHADPA LAN IPV4 DAN LAN IPV6

Bungur Togi Andre Sihotang[1], Niken Dwi Cahyani[2], Asep Mulyana[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Sebagai salah satu jenis serangan terhadap sistem komputer, Denial of service senantiasa berkembang dalam berbagai bentuk. Perbedaan utama dengan jenis serangan lain adalah bahwa vulnerability yang diincar bukan data yang dikirimkan, melainkan sistem yang mengirim dan menerima data. Pada penelitian ini Denial of service akan diujicobakan terhadap LAN sederhana terdiri dari 3 kompuiter dengan sistem operasi Windows yang mendukung dua protokol masing-masing IPv4 dan IPv6. Dimana IPv4 merupakan model pengalamatan yang umum dipakai sampai saat ini dan IPv6 merupakan model pengalamatan terbaru yang diproyeksikan menggantikan IPv4 di masa mendatang. Parameter yang digunakan diutamakan dari sisi user yakni response time, transfer time, dan throughput. Serangan dan pengukuran parameter dilakukan secara terpisah untuk pengalamatan IPv4 dan IPv6.

Dari hasil percobaan dapat diketahui bahwa umumnya serangan Denial of service yang diujicobakan memberikan dampak yang negative bagi layanan pada LAN tersebut namun tidak terlalu besar karena LAN yang memang hanya memiliki sedikit komputer. Kemudian dari analisis perbandingan untuk dua pengalamatan yang dipakai, LAN dengan IPv6 sedikit lebih baik secara partial daripada LAN IPv4, tetapi ada juga layanan yang boleh dikatakan tidak ada perbedaan bila menggunakan IPv4 maupun IPv6 bila dilihat dari sisi user. Oleh karena itu, hasil penelitian ini belum dapat memberikan pertimbangan yang spesifik dalam memutuskan pembangunan LAN dengan pengalamatan tertentu, tetapi diharapkan cukup sebagai sebuah referensi yang baik ke depannya.

Kata Kunci : Denial of service (DoS), Local Area Network, dual stack, Windows, IPv4, IPv6, response time, transfer time, throughput

Abstract

As one of the network threats, Denial of service always spread into one and many variations. The main differentiation between Denial of service and other threats is the vulnerability that Denial of service try to attack is the sistem in which the data are transferred, not the particular data. In this research, Denial of service will be tried to observe by done it on a simple Local Area Network consists of three computers use Windows operating system that supports both IPv4 and IPv6 protocols. IPv4 is the current network addressing model that many systems use nowadays and IPv6 is the other network addressing model that is predicted to replace IPv4 in the near future. Paramaters which are used in this research are relatively make sense for user consist of response time, transfer time, jitter, and throughput. The attack experiment and process of determining parameters above will be separated into both network addressing models, IPv4 and IPv6.

From the experiment, it could be known that the impacts on the services given by Denial of service is certainly negative but they are relatively not too big as the Local Area Network here only consist of a small number of computers. Then from the comparition analysis between these two addressing models, we can gain that IPv6 network is a little bit better for some particular services than IPv4 network, but in the other hand some services do not show any respectable differences for user between these two ones. So the results from this research should not be used particularly for a network development and to decide which addressing model might be used, as there area many aspects should be noticed in this case. But at least this experiment could be used as an useful reference.

Keywords : Denial of service (DoS), Local Area Network, dual stack, Windows, IPv4, IPv6, response time, transfer time, throughput

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pertumbuhan jumlah pengguna Internet sangat pesat dalam satu dekade terakhir. Hal ini membuat jumlah alamat *IP address* global yang merupakan protokol pengalamatan *IP version 4* (IPv4) semakin menipis. Kekhawatiran ini membuat para ahli jaringan komputer merancang suatu protokol pengalamatan terbaru yaitu *IP version 6* (IPv6). Protokol yang berada di bawah layer *network* pada standar OSI Layer ini memang belum diiplementasikan secara menyeluruh pada sistem komputer di seluruh dunia, namun perlahan-lahan mulai diimplementasikan, contohnya pada sistem operasi Windows Vista dimana IPv6 sudah dapat diinstall pada komputer dan Linux yang sudah mendukung IPv6. Dengan ketersediaan jumlah alamat IP yang sangat banyak (2^{128}), diharapkan IPv6 dapat mendukung pertumbuhan pengguna Internet di seluruh dunia.

Dalam implementasinya sekarang, IPv6 banyak dijadikan bahan kajian penelitian maupun percobaan karena diperkirakan baru sekitar 5-10 tahun lagi IPv6 dipakai menggantikan IPv4 secara menyeluruh. Untuk saat ini umumnya alamat IPv6 masih dipakai secara berdampingan dengan alamat IPv4 yang masih luas digunakan. Salah satu aspek penelitian yang banyak dikaji adalah mengenai jalannya aplikasi di atas alamat IPv6 serta aspek keamanan jaringan yang menggunakan pengalamatan IPv4 dan IPv6. Jenis-jenis jaringan pun bisa bermacam yaitu jaringan global (Internet), *Wide Area Network* (WAN), dan *Local Area Network* (LAN). Berangkat dari situlah maka penelitian ini dilakukan dengan tujuan untuk mengetahui dampak yang ditimbulkan oleh salah satu serangan yaitu *Denial of service* (DoS) terhadap aplikasi-aplikasi pada jaringan LAN yang menggunakan alamat IPv4 dan alamat IPv6.

Pada percobaan ini akan dibuat dua skenario percobaan yaitu menjalankan aplikasi dengan pengalamatan menggunakan protokol IPv4 untuk skenario pertama dan skenario kedua aplikasi dengan pengalamatan IPv6. Sistem operasi yang digunakan adalah Windows Server 2008 dan Windows Vista yang dipakai pada tiga buah komputer yang akan dijadikan LAN dan telah mendukung kedua pengalamatan tersebut. Kemudian akan dicoba untuk melancarkan beberapa jenis serangan DoS dengan kedua skenario tersebut. Setelah itu akan diukur dampak yang terjadi pada kedua skenario melalui beberapa parameter yang telah ditentukan. Akan dilihat dan dianalisis apakah dampak serangan pada kedua skenario relatif sama, berbeda jauh, atau berbeda tetapi tidak terlalu besar. Analisis perbandingan akan dilihat dari dampak terhadap *user* karena yang ingin ditekankan melalui hasil penelitian ini adalah dampak terhadap *user* saat mengakses dan memanfaatkan aplikasi pada jaringan.

1.2 Rumusan Masalah

Pada tugas akhir kali ini akan dilakukan analisis terhadap hasil ujicoba serangan DoS pada dua skenario *Local Area Network* (LAN). Secara garis besar, kerangka perumusan masalah dijabarkan dalam beberapa poin berikut ini :

a. Merancang sebuah LAN yang dapat mengimplementasikan dua buah protokol pengalamatan yaitu IPv4 dan IPv6 (*dual stack*) beserta aplikasi yang telah mendukung kedua pengalamatan tersebut yaitu aplikasi web, FTP, dan streaming.
b. Melakukan serangan DoS terhadap LAN yang telah dirancang sebelumnya dan menganalisis dampak serangan tersebut terhadap LAN. Analisis dilakukan dengan cara mengukur parameter *response time, transfer time, dan throughput* pada kedua skenario percobaan yaitu menjalankan aplikasi yang menggunakan alamat IPv4 dan alamat IPv6 saat serangan DoS dilakukan.
c. Bagaimana perbandingan hasil percobaan antara kedua skenario percobaan di atas? Mengapa diperoleh hasil percobaan demikian?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dalam tugas akhir ini adalah :

a. Membangun sebuah jaringan LAN terdiri dari 3 *host* dihubungkan dengan switch yang menggunakan dua protokol pengalamatan sekaligus yaitu protokol IPv4 atau IPv6 (*dual stack*).
b. Menganalisis dampak yang ditimbulkan tiap serangan DoS pada aplikasi dan kondisi yang bersesuaian melalui pengukuran parameter *response time, transfer time,* dan *throughput* pada saat terjadi serangan untuk masing-masing skenario percobaan.
c. Membandingkan dan menganalisis dampak serangan yang merupakan hasil percobaan dari kedua skenario percobaan tersebut untuk kemudian diambil kesimpulan yang nantinya dapat dijadikan referensi bagi pembangunan sebuah jaringan lokal

1.4 Batasan Masalah

Adapun dalam tugas besar kali ini ada beberapa batasan masalah yaitu:

a. LAN yang dibangun menggunakan *Fast Ethernet* 100 MBps, terdiri dari 3 *host*, dan tidak terhubung ke jaringan lain termasuk ke Internet.
b. Sistem Operasi yang digunakan adalah Windows Server 2008 dan Windows Vista Konfigurasi aplikasi dan sistem operasi adalah sama untuk kedua skenario percobaan pada tiap *host* kecuali pengalamatan (*IP Address*)

c. Jenis serangan DoS yang dilakukan sesuai dengan definisi dan pengkategorian DoS pada dokumen *Cert.org* dan disesuaikan dengan kondisi LAN yang sederhana, menggunakan switch, dan tidak terhubung ke jaringan lain.
d. Serangan dibagi dua kategori berdasarkan lokasi penyerangan, yaitu serangan yang dilakukan dari dalam komputer server itu sendiri dan serangan yang dilakukan melalui salah satu komputer (klien2) terhadap komputer server.
e. Pengukuran parameter dilakukan secara manual dengan ketelitian sampai dua angka di belakang koma sesuai dengan kemampuan pengamatan mata manusia. Perbedaan dampak akan dilihat dari level satu angka di depan koma.
f. Aplikasi dalam jaringan yang dimiliki berupa website, *File Transfer Protocol* dan *streaming* dimana ketiganya telah mendukung pengalamatan IPv4 dan IPv6
g. Pada percobaan ini tidak digunakan tools keamanan jaringan eksternal / tambahan seperti *Sentinel*, *Integrity Server*, *Intrusion Detection System*, dan sebagainya.

1.5 Metodologi Penelitian

Metode penelitian yang dilakukan untuk implementasi tersebut adalah :

1. Studi Literatur

   Pada tahap ini akan dilakukan pendalaman konsep dan teori dengan mempelajari literatur-literatur yang relevan dengan permasalahan yang meliputi

   - Jaringan LAN dan TCP/IP.
   - Serangan *Denial of service*
   - IPv4 dan IPv6
   - *Quality of Service* (QoS).

2. Perancangan Jaringan

   Pada tahap ini akan dilakukan pembangunan jaringan LAN yang akan diujicobakan lengkap dengan *hardware* dan instalasi *software* yang dibutuhkan yaitu web server (*Internet Information Service 7.0*), FTP server (*Xlight FTP Server*) dan streaming server (*VLC Media Player*)

3. Implementasi

   Setelah jaringan terbangun, kemudian serangan *Denial of service* dilancarkan pada kedua skenario. Kemudian akan dilakukan pengukuran dampak dari serangan tersebut melalui aplikasi pada jaringan yang diakses oleh *user* untuk masing-masing skenaro. Skenario pertama yaitu LAN yang hanya menggunakan pengalamatan IPv4 (*IPv4 only*). Kemudian skenario kedua yaitu LAN yang hanya menggunakan pengalamatan IPv6 (*IPv6 only*). Kedua skenario tersebut dilakukan pada LAN dengan tiga komputer, dimana server

menggunakan sistem operasi Windows Server 2008 dan kedua klien menggunakan Windows Vista

4. Analisis Perbandingan

   Setelah percobaan dilakukan, kemudian hasil percobaan dipisahkan antara skenario pertama dengan skenario kedua untuk dilakukan analisis perbandingan. Dari hasil analisis tersebut kemudian akan ditarik kesimpulan.

5. Penyusunan Laporan Tugas Akhir.

1.6 Sistematika Penulisan

Tugas akhir ini disusun dengan sistematika penulisan sebagai berikut :

BAB I Pendahuluan

Bab ini menguraikan tugas akhir ini secara umum, meliputi latar belakang, perumusan masalah, tujuan, batasan masalah, dan sistematika penulisan

BAB II Landasan Teori

Bab ini membahas mengenai uraian teori yang berhubungan dengan layer aplikasi, layer *network* dimana IPv4 dan IPv6 didefinisikan, serangan *Denial of service*, dan parameter pengujian yang digunakan yaitu *response time, transfer time, dan throughput.*

BAB III Perancangan

Bab ini berisi latar belakang pembangunan sistem, kebutuhan hardware sistem, skenario jaringan dan aplikasi di dalamnya, serta proses instalasi dan konfigurasi.pengalamatan

BAB IV Pengujian

Bab ini membahas mengenai latar belakang dan tata cara pengujian yang dilakukan serta langkah-langkah yang dilakukan selama pengujian berupa detail setiap serangan DoS yang dilakukan dan cara pengukuran dampaknya. Dalam hal ini LAN dibagi dua skenario yaitu skenario pertama dimana kopmuter-komputer pada LAN hanya menggunakan pengalamatan IPv4, sedangkan pada skenario kedua hanya menggunakan pengalamatn Ipv6

BAB V Analisis Perbandingan Hasil Pengujian

Bab ini berisi analisis perbandingan antara hasil percobaan antara skenario pertama dan skenario kedua berikut gambar yang menampilkan perbandingan hasil percobaan secara visual.

BAB VI Kesimpulan dan Saran

Berisi kesimpulan dari penulisan Tugas Akhir ini dan saran-saran yang diperlukan untuk pengembangan penelitian lebih lanjut.

BAB 6
KESIMPULAN DAN SARAN

6.1. Kesimpulan

1. Secara umum dampak dari setiap serangan yang dilancarkan terhadap jaringan tidak terlalu besar. Dikarenakan jumlah *host* yang sedikit serta kapasistas jaringan dalam hal ini lebar *bandwidth* (*Fast Ethernet* 100 MBps) serta kecepatan pemrosesan baik pada *node* server maupun klien yang sangat cepat (LAN). Selain itu serangan yang hanya dilancarkan dari satu *host* tidak berdampak besar bagi jalannya aplikasi pada LAN ini.
2. Ditinjau dari perbandingan pengukuran *response time*, aplikasi-aplikasi di atas pengalamatan IPv6 tidak berbeda jauh dengan pengalamatan IPv4. Ini mungkin dikarenakan pemrosesan paket IPv4 dan IPv6 pada sistem operasi Windows Server 2008 dan Windows Vista sudah diimplementasikan secara penuh. Selain itu bandwith yang lebar (*Fast Ethernet* 100 MBps) dan jumlah *host* yang sedikit membuat waktu loading aplikasi cukup cepat.
3. Ditinjau dari parameter *transfer time*, aplikasi-aplikasi di atas pengalamatan IPv6 berjalan sedikit lebih baik. Ini dikarenakan pemrosesan paket pada saat transfer data di IPv6 yang lebih sederhana dibandingkan IPv4 sehingga akan memberikan waktu yang lebih kecil pada jumlah paket data yang sangat banyak. Namun, dari hasil pengujian serangan memberikan dampak walaupun tdiak terlalu besar dan dapat dikatakan perbedaannya tidak terlalu signifikan dikarenakan karakteristik LAN itu sendiri serta daya serangan yang hanya berasal dari satu *host* saja.
4. Ditinjau dari *throughput*, bahwa aplikasi-aplikasi di atas skenario pengalamatan IPv6 memiliki *throughput* yang lebih baik dibandingkan dengan IPv4. Karena parameter *transfer time* berbanding lurus dengan *throughput*. Untuk LAN pada penelitian ini, tentu perbedaan ini tidak terlalu berpengaruh signifikan karena aktivitas transfer data yang relatif tidak besar (kisaran puluhan – ratusan *megabyte*). Namun, ini tentu akan sangat bermanfaat dalam suatu perusahaan atau organisasi yang memiliki aktivitas transfer data dalam jumlah dan frekuensi yang besar serta skala jaringan yang luas.
5. Ditinjau dari perbandingan parameter-parameter yang diukur pada percobaan serangan *Denial of service*, kedua skenario LAN yaitu IPv6 dan IPv4 relatif tidak jauh berbeda jauh bila dilihat dari sisi *user* (pendekatan hingga dua angka di belakang koma). Namun menyangkut *business value* ini tentu berpengaruh bila jumlah *host* dalam jaringan sangat besar sehingga perbedaan *transfer*

time dan *throughput* akan berdampak bagi efektivitas dan *cost* sebuah perusahaan. Keberadaan Sistem Operasi Server 2008 dan Windows Vista yang telah mengimplementasikan kedua protokol pengalamatan tersebut terbukti membuat penggunaan masing-masing pengalamatan berjalan lebih baik dan akhirnya mendukung jalannya aplikasi pada sistem.

6. Dengan mempertimbangkan hal-hal di atas, hasil penelitian ini belum dapat digunakan secara parsial atau dijadikan pertimbangan utama untuk menentukan kebijakan protokol pengalamatan apa yang dapat dipakai, karena banyak aspek lain yang harus dipertimbangkan berhubungan dengan *user* seperti *cost*, sistem operasi, skalabilitas jaringan, dukungan infrastruktur, pelatihan *user* mengenai IPv6, sumber daya manusia, dsb.
7. Pada akhirnya keputusan untuk menggunakan sebuah pengalamatan apakah IPv4 ataupun IPv6 bila ditinjau dari sisi *user* dan bisnis tentu harus melibatkan aspek-aspek yang lainnya. Namun bukan berarti IPv6 tidak perlu digunakan karena melihat dari prediksi para ahli jaringan komputer bahwa sekitar 5 tahun ke depan IPv6 akan semakin banyak digunakan untuk menggantikan pengalamatan IPv4. Tentunya akan lebih baik bila hal tersebut dapat dipertimbangkan dan dipersiapkan lebih dini.

6.2. Saran

1. Untuk penelitian selanjutnya, diharapkan media pengujian atau penelitian yang digunakan dapat lebih besar dalam arti jumlah komputer yang lebih banyak. Selain itu jaringan juga bisa terdiri dari beberapa jaringan kecil yang dihubungkan menggunakan *PC Router* sehingga dapat digunakan untuk membandingkan implementasi penggunaan protokol IPv4 dan IPv6.
2. Salah satu serangan *Denial of service* yang beberapa tahun lalu menarik perhatian banyak kalangan yakni *Distributed Denial of service* (DDoS), hanya saying sekali tidak dapat diujicobakan pada penelitian ini karena keterbatasan sarana. DDoS bisa diteliti, untuk kemudian diujicobakan dan dianalisis dalam sebuah topik penelitian yang baru. Akan lebih baik bila beberapa solusi yang telah diangkat ke dalam paper atau esai dapat diujicobakan juga dalam menghadapi serangan DDoS ini.
3. Beberapa teknik mengamankan sistem komputer untuk menghadapi serangan *Denial of service* dan berbagai macam serangan keamanan lainnya telah bermunculan dan diwacanakan ke dalam paper atau seminar tanpa adanya publikasi mengenai implementasinya. Mungkin beberapa dari teknik tersebut dapat diangkat menjadi sebuah topik penelitian yang baru khusus mengenai serangan *Denial of service*.

Daftar Pustaka

[1] Basalamah A. *TCP/IP Insecurity*. Computer Network Research Group (CNRG) Microelectronics System Application Lab, Inter University Center on Microelectronics. Indonesia : Institute of Technology Bandung

[2] CERT® Coordination Center. 2001. *Denial of Service Attacks*. USA : Carnegie Mellon University. Sumber internet : *http://www.cert.org*

[3] Davies, Joseph. *Internet Protocol version 6 transition technologies*. November 2006 : Technical writer Windows Networking and Device Technologies, Microsoft Corporation

[4] de Lattre A., Bilien J., Daoud A, Stenac C., Cellerier A., Saman J.P. *VideoLAN Streaming Howto*. 2005. VideoLAN Project

[5] Dewo E.S. *Bandwidth dan Throughput*. 2003. *http://www.ilmukomputer.com*

[6] Handley, Rescorla. 2006. *RFC 4732 - Internet Denial-of-Service Considerations*. The IETF Trust.

[7] Houle, Weaver. CERT® Coordination Center. 2001. *Trends in Denial of ServiceAttack Technology*. USA : Carnegie Mellon University.

[8] *http://www.securityfocus.com*

[9] Husman, Hans. “Introduction to Denial of Service”, *t95hhu@student.tdb.uu.se*

[10] *Introduction to IP Version 6*. January 2008 : Microsoft Corporation

[11] Lammle, Todd. 2005. *Cisco Certified Network Associate : Study Guide*, Elex Media Komputindo. Jakarta.

[12] Packet Storm Security. http://www.packetstromsecurity.org

[13] Planet Source Code. http://www.planet-source-code.com

[14] Purbo, Onno W. *Ensiklopedia Denial of Service*.2001:*PC Magazine* http://205.181.113.18/pcmag/pctech/content/17/08/nt1708.002.html

[15] The Cable Guy. 2005. *Changes to IPv6 in Windows Vista and Windows Server 2008*. Microsoft Corporation

[16] WSS-ID Team. 2007. *Windows Server 2008 Panduan Praktis untuk Administrator*. Jakarta. Majalah Info Komputer Pt. Prima Infosarana Media Gramedia

[17] Xlight FTP Server - *Frequency Asked Questions*. XLight FTP Project http://www.xlightftpd.com/faq.htm.