

ANALISIS DAMPAK SERANGAN *DENIAL OF SERVICE* TERHADAP *WEB SERVER* BERBASIS *WINDOWS*

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan
Program Strata 1, Program Studi Teknik Informatika,
Universitas Pasundan Bandung

Oleh :

Muhammad Fariz Faizal
Nrp. 10.304.0100



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
JUNI 2017**

LEMBAR PENGESAHAN LAPORAN TUGAS AKHIR

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari dan tanggal sidang sesuai berita acara sidang, tugas akhir dari :

Nama : Muhammad Fariz Faizal
Nrp : 10.304.0100

Dengan judul :

“ANALISIS DAMPAK SERANGAN *DENIAL OF SERVICE* TERHADAP *WEB SERVER* BERBASIS *WINDOWS*”

Bandung, 8 Juni 2017

Menyetujui,

Pembimbing Utama,

Pembimbing Pendamping,

(Doddy Ferdiansyah, S.T, M.T)

(Ferry Mulyanto, ST., M.Kom)

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

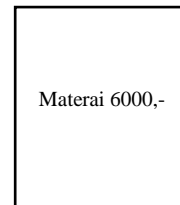
Saya menyatakan dengan sesungguhnya bahwa :

1. Tugas Akhir ini adalah benar – benar asli dan belum pernah diajukan untuk mendapatkan gelar akademik, baik di Universitas Pasundan Bandung maupun di Perguruan Tinggi lainnya.
2. Tugas Akhir ini adalah gagasan, rumusan dan penelitian saya sendiri, tanpa bantuan pihak lain kecuali arahan dari tim Dosen Pembimbing.
3. Dalam Tugas Akhir ini tidak terdapat karya atau pendapat orang lain, kecuali bagian – bagian tertentu dalam penulisan laporan Tugas Akhir yang saya kutip dari karya orang lain telah dituliskan dalam sumbernya secara jelas sesuai dengan norma, kaidah, dan etika penulisan karya ilmiah, serta disebutkan dalam Daftar Pustaka pada tugas akhir ini.
4. Kakas, perangkat lunak, dan alat bantu kerja lainnya yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab Universitas Pasundan Bandung.

Apabila di kemudian hari ditemukan seluruh atau sebagian laporan tugas akhir ini bukan hasil karya saya sendiri atau adanya plagiasi dalam bagian – bagian tertentu, saya bersedia menerima sanksi akademik, termasuk pencabutan gelar akademik yang saya sandang sesuai dengan norma yang berlaku di Universitas Pasundan, serta perundang – undangan lainnya.

Bandung, 8 Juni 2017

Yang membuat pernyataan,



(Muhammad Fariz Faizal)

NRP. 10.304.0100

ABSTRAK

Perkembangan internet yang semakin cepat dan canggih dengan berbagai macam fungsi dan kebutuhan menuntut meningkatnya kualitas keamanan jaringan *web server*. Terutama dengan semakin terbukanya pengetahuan *hacking* dan *cracking*, didukung dengan banyaknya *tools* yang tersedia dengan mudah dan *free*, semakin mempermudah *attacker* untuk melakukan penyusupan atau serangan.

Serangan *Denial of Service* terhadap *web server* berbasis *windows* yaitu *web server apache* dan *web server IIS* dapat menimbulkan *traffic / request flooding* terhadap *web server*, sehingga dapat menimbulkan masalah pada aspek ketersediaan (*availability*). Aspek ketersediaan (*availability*) yaitu aspek yang menjamin bahwa data akan tersedia saat dibutuhkan oleh pengguna.

Pada penelitian tugas akhir ini, penulis melakukan pengujian terhadap *web server* berbasis *windows* yaitu *web server apache* dan *web server IIS* dengan menggunakan metode *denial of service* untuk mendapatkan hasil berupa informasi dampak serangan *denial of service* terhadap *web server apache* dan *web server IIS*. Setelah melakukan pengujian, maka terdapat manfaat dan solusi yaitu rekomendasi kaskas keamanan yang sesuai dari dampak serangan *denial of service* terhadap *web server* berbasis *windows*.

Kata Kunci: *Web Server, Apache, IIS (internet information services), DoS, Traffic Flooding, Request Flooding*

ABSTRACT

The development of increasingly faster internet and sophisticated with a wide range of functions and needs of demanding improved quality of network security of the web server. Especially with the opening of the knowledge of hacking and cracking, is supported by the many tools available with easy and free, make it easier for attackers to infiltrate or attack.

Denial of Service attacks against Windows-based web server is a web server Apache and IIS web server can generate traffic / request flooding to the web server, so it can cause problems in the aspect of availability. Aspects of availability are aspects that guarantee that data will be available when needed by the user.

In this research, the authors tested the Windows-based web server is a web server Apache and IIS web servers using the method of denial of service to get the information in the form of the impact of denial of service attacks against web servers Apache and IIS web server. After a test, then there are benefits and solutions that appropriate security Kakas recommendations of the impact of denial of service attacks against Windows-based web server.

Keyword: Web Server, Apache, IIS (internet information services), DoS, Traffic Flooding, Request Flooding

KATA PENGANTAR



Puji dan syukur penulis panjatkan kehadiran Allah SWT karena berkat rahmat dan karunia-Nya, penulis dapat menyelesaikan Tugas Akhir ini yang berjudul “Analisis Dampak Serangan *Denial of Service* Terhadap *Web Server* Berbasis *Windows*”. Tugas akhir ini diajukan untuk memenuhi salah satu syarat dalam menempuh kelulusan Stara 1 Program Teknik Informatika, Fakultas Teknik Universitas Pasundan Bandung. Penulis menyadari bahwa penyusunan Tugas Akhir ini masih banyak terdapat kekurangan dan masih jauh dari kesempurnaan, hal ini dikarenakan keterbatasan kemampuan yang penulis miliki.

Atas segala kekurangan dan ketidaksempurnaan Tugas Akhir ini, penulis sangat mengharapkan masukan, kritik dan saran yang bersifat membangun kearah perbaikan dan penyempurnaan Tugas Akhir ini. Cukup banyak kesulitan yang penulis temui dalam penulisan Tugas Akhir ini, tetapi Alhamdulillah dapat penulis atasi dan selesaikan dengan baik. Akhir kata penulis berharap semoga Tugas Akhir ini dapat bermanfaat bagi semua pihak dan semoga amal baik yang telah diberikan kepada penulis mendapat balasan dari Allah SWT.

Bandung, 8 Juni 2017

Penulis

UCAPAN TERIMAKASIH

Selama menyelesaikan penyusunan Tugas Akhir ini penulis telah banyak dibantu oleh berbagai pihak, baik secara langsung maupun tidak langsung. Untuk itu, dengan segala kerendahan hati, penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang turut membantu, khususnya :

1. Seluruh keluarga besar yang senantiasa memberikan doa, motivasi, dan dukungan penulis terhadap pengerjaan tugas akhir.
2. Bapak ShandikaGalih Amalga, ST., MT. selaku dosen wali yang telah membimbing dan menjadi dosen wali penulis selama masa perkuliahan.
3. Bapak Doddy Ferdiansyah, S.T, M.T selaku dosen pembimbing utama serta bapak Ferry Mulyanto, ST., M.Kom pembimbing kedua yang sudah membantu banyak kepada penulis untuk menyelesaikan tugas akhir ini.
4. Bapak Sali Alas Majapahit, S.ST., M.KOM., selaku Koordinator Tugas akhir.
5. Dosen – dosen beserta staff Teknik Informatika Universitas Pasundan atas ilmu dan pelajarannya yang selama ini penulis dapatkan.
6. Semua teman-teman seperjuangan Teknik Informatika angkatan 2010 serta rekan-rekan penulis tidak bisa penulis tuliskan semua yang telah membantu memberikan saran dan semangat dalam mendukung penulis dalam menyelesaikan tugas akhir ini.

Bandung , 8 Juni 2017

Penulis

DAFTAR ISI

ABSTRAK.....	i
ABSTRACT.....	ii
KATA PENGANTAR	iii
UCAPAN TERIMAKASIH	iv
DAFTAR ISI.....	v
DAFTAR ISTILAH	vii
DAFTAR TABEL.....	viii
DAFTAR LAMPIRAN	xii
DAFTAR SIMBOL.....	xiii
BAB 1 PENDAHULUAN	1-1
1.1 Latar Belakang	1-1
1.2 Identifikasi Masalah	1-2
1.3 Tujuan Tugas Akhir	1-2
1.4 Lingkup Tugas Akhir	1-2
1.5 Metodologi Tugas Akhir	1-3
1.6 Sistematika Penulisan	1-4
BAB 2 LANDASAN TEORI.....	2-1
2.1 Definisi Dampak	2-1
2.2 Keamanan Informasi	2-1
2.3 Web Server	2-2
2.4 Denial of Service (DOS)	2-4
2.5 Honeypot.....	2-8
2.5.1 Jenis Honeypot.....	2-8
2.6 Anatomy of Hack	2-10
2.7 Penelitian Terdahulu	2-11
BAB 3 SKEMA PENELITIAN	3-1
3.1 Peta Konsep	3-1
3.2 Rancangan Penelitian	3-1
3.3 Rencana Analisis.....	3-3
3.3.1 Peta Analisis	3-4
3.4 Analisis Kebutuhan Penelitian	3-5

3.4.1 Pemahaman Web Server Apache	3-5
3.4.2 Pemahaman Web Server IIS.....	3-6
3.4.3 Analisis Kebutuhan <i>Hardware</i>	3-7
3.4.4 Analisis Kebutuhan <i>Software</i>	3-7
3.5 Skenario Uji Coba	3-8
3.5.1 Topologi Jaringan.....	3-9
3.6 Analisis Solusi.....	3-9
3.6.1 Analisis Masalah	3-9
3.6.2 Peran Penelitian.....	3-10
3.6.3 Analisis manfaat penelitian	3-10
3.6.4 Kerangka Pemikiran Teoritis.....	3-10
3.6.5 Analisis Hasil Pengujian Web Server Apache dan Web Server IIS.....	3-11
BAB 4 IMPLEMENTASI DAN PENGUJIAN	4-1
4.1 Skenario Pengujian.....	4-1
4.2 Tahap – Tahap Skenario Pengujian	4-1
4.3 Lingkungan Pengujian.....	4-2
4.4 Pengujian Web Server	4-3
4.4.1 Pengujian <i>Web Server Apache</i> Versi 2.4	4-5
4.4.2 Pengujian Web Server Apache Versi 2.2.19.....	4-17
4.4.3 Pengujian Web Server IIS Versi 8.....	4-28
4.4.4 Pengujian Web Server IIS Versi 10.....	4-28
4.5 Hasil Analisis Dampak Serangan <i>Denial of Service</i> terhadap <i>Websserver</i> berbasis <i>Windows</i>	4-39
4.6 Karakteristik <i>Tools Denial of Service</i>	4-44
4.7 Manfaat Analisis Dampak Serangan Denial of Service	4-44
4.8 Rekomendasi Kakas Keamanan	4-44
BAB 5 KESIMPULAN DAN SARAN	5-1
5.1 Kesimpulan	5-1
5.2 Saran	5-1
DAFTAR PUSTAKA	xv
LAMPIRAN.....	xvi

DAFTAR ISTILAH

Berikut dibawah ini adalah istilah – istilah yang terdapat didalam laporan analisis dampak serangan *denial of service* terhadap *web server* berbasis *windows*.

Nama Istilah	Deskripsi
<i>DOS (Denial of Service)</i>	Serangan pada sebuah server atau komputer yang menghabiskan resource dari computer tersebut
<i>Firewall</i>	sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman
<i>honeypot</i>	suatu cara untuk menjebak atau menangkai usaha-usaha penggunaan tak terotorisasi dalam sebuah sistem informasi
<i>IDS (Intrusion Detection System)</i>	sebuah metode yang dapat digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan
<i>Web server</i>	sebuah software yang memberikan layanan berbasis data dan berfungsi menerima permintaan dari HTTP atau HTTPS
<i>Apache</i>	Sebuah nama web server yang bertanggung jawab pada request-response HTTP dan logging informasi secara detail(kegunaan dasarnya)
<i>lis (Internet Information Services)</i>	sebuah HTTP web server yang digunakan dalam sistem operasi server Windows
<i>Kali linux</i>	Generasi baru dari BackTrack Linux, pemimpin industri Penetration Testing dan audit keamanan distribusi Linux
<i>Windows</i>	keluarga sistem operasi yang dikembangkan oleh Microsoft, dengan menggunakan antarmuka pengguna grafis
<i>Penetration</i>	Metode untuk mengevaluasi keamanan sistem computer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya
<i>Botnet</i>	botnet adalah sekumpulan program yang saling terhubung melalui Internet yang berkomunikasi dengan program-program sejenis untuk melakukan tugas tertentu. Botnet bisa dipakai untuk menjaga keamanan kanal IRC, mengirimkan surel spam, atau berpartisipasi dalam serangan DDos.
<i>CPU (Central Processing Unit)</i>	<i>CPU (Central Processing Unit)</i> adalah otak atau sumber dari komputer yang mengatur dan memproses seluruh kerja computer.
<i>IP (Internet Protocol)</i>	Alamat IP (<i>Internet Protocol Address</i> atau sering disingkat IP) adalah deretan angka biner antara 32 bit sampai 128 bit yang dipakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan Internet.

DAFTAR TABEL

Tabel 2.1 Perbandingan Serangan Denial Of Service [SBI04]	2-8
Tabel 2.2 Penelitian Terdahulu.....	2-11
Tabel 3.1 Penjelasan Skema Analisis	3-4
Tabel 3.2 Dampak serangan denial of service terhadap web server apache dan web server iis	3-11
Tabel 4.1 Dampak serangan XerXes terhadap web server apache versi 2.4	4-10
Tabel 4.2 Dampak serangan Apachekiller terhadap web server apache versi 2.4	4-13
Tabel 4.3 Dampak serangan HULK terhadap web server apache versi 2.4	4-16
Tabel 4.4 Dampak serangan XerXes terhadap web server apache versi 2.2.19	4-21
Tabel 4.5 Dampak serangan <i>Apachekiller</i> terhadap <i>webservice apache</i> versi 2.2.19.....	4-24
Tabel 4.6 Dampak serangan HULK terhadap web server apache versi 2.2.19	4-27
Tabel 4.7 <i>Internet information services compatibility</i>	4-28
Tabel 4.8 <i>Dampak serangan XerXes terhadap web server iis versi 10</i>	4-32
Tabel 4.9 Dampak serangan Apachekiller terhadap web server iis versi 10	4-35
Tabel 4.10 Dampak serangan HULK terhadap web server iis versi 10.....	4-37
Tabel 4.11 Hasil Analisis Serangan DOS terhadap webservice apache dan webservice iis	4-39
Tabel 4.12 Perbandingan Dampak Serangan Denial of Service.....	4-44

DAFTAR GAMBAR

Gambar 1.1 Hasil Survey Webserver oleh Netcraft.....	1-1
Gambar 1.2 Metodologi Tugas Akhir.....	1-3
Gambar 2.1 Keamanan Informasi.....	2-2
Gambar 2.2 Skema program utility ping dan serangan Ping of Death [SBI04]	2-5
Gambar 2.3 skema koneksi TCP three-way handshake [SBI04]	2-6
Gambar 2.4 Skema Serangan SYN [SBI04]	2-6
Gambar 2.5 Skema Serangan LAND [SBI04]	2-7
Gambar 2.6 Skema Serangan Smurf Attack [SBI04].....	2-7
Gambar 2.7 Contoh penempatan honeypot padai jaringan [SPI02]	2-8
Gambar 3.1 Peta Konsep	3-1
Gambar 3.2 Kerangka Tugas Akhir - 1.....	3-2
Gambar 3.3 Kerangka Tugas Akhir - 2.....	3-3
Gambar 3.4 Skema Analisis	3-4
Gambar 3.5 Survey Web Server Apache [NET17].....	3-6
Gambar 3.6 Survey Web Server IIS [NET17]	3-6
Gambar 3.7 Skenario Uji Coba.....	3-8
Gambar 3.8 Topologi Jaringan	3-9
Gambar 3.9 Kerangka Pemikiran Teoritis	3-11
Gambar 4.1 Skenario Pengujian	4-1
Gambar 4.2 Tahap Scanning	4-2
Gambar 4.3 Tahap Penetration	4-2
Gambar 4.4 Akses Website Localhost (Apache 2.4)	4-3
Gambar 4.5 Akses Website Localhost (Apache 2.2.19)	4-4
Gambar 4.6 Akses Website Localhost (IIS 10).....	4-4
Gambar 4.7 Kinerja CPU (Kondisi Normal)	4-5
Gambar 4.8 Lalu Lintas Paket Data (Kondisi Normal).....	4-5
Gambar 4.9 Hasil Scanning Apache versi 2.4	4-6
Gambar 4.10 Proses Apache Sebelum Penyerangan.....	4-6
Gambar 4.11 Lalulintas Paket Data Sebelum Penyerangan	4-7
Gambar 4.12 Perintah XerXes.....	4-7
Gambar 4.13 Proses Penyerangan XerXes	4-8
Gambar 4.14 Akses Website Setelah Penyerangan XerXes.....	4-8
Gambar 4.15 Kinerja CPU Setelah Penyerangan XerXes.....	4-9
Gambar 4.16 Lalu Lintas Paket Data Setelah Penyerangan XerXes - 1.....	4-9
Gambar 4.17 Lalu Lintas Paket Data Setelah Penyerangan XerXes - 2.....	4-10
Gambar 4.18 Perintah Apachekiller	4-11

Gambar 4.19 Proses Penyerangan Apachekiller	4-11
Gambar 4.20 Akses Website Setelah Penyerangan Apachekiller	4-12
Gambar 4.21 Kinerja CPU Setelah Penyerangan Apachekiller	4-12
Gambar 4.22 lalu Lintas Paket Data Setelah Penyerangan Apachekiller	4-13
Gambar 4.23 Perintah HULK.....	4-14
Gambar 4.24 Akses Website Setelah Penyerangan HULK.....	4-14
Gambar 4.25 Kinerja CPU Setelah Penyerangan HULK.....	4-15
Gambar 4.26 Lalu Lintas Paket Data Setelah Penyerangan HULK - 1.....	4-15
Gambar 4.27 Lalu Lintas Paket Data Setelah Penyerangan HULK – 2.....	4-16
Gambar 4.28 Hasil Scanning Apache versi 2.2.19	4-17
Gambar 4.29 Proses Apache Sebelum Penyerangan	4-17
Gambar 4.30 Lalulintas Paket Data Sebelum Penyerangan	4-18
Gambar 4.31 Perintah XerXes.....	4-18
Gambar 4.32 Proses Penyerangan XerXes	4-19
Gambar 4.33 Akses Website Setelah Penyerangan XerXes	4-19
Gambar 4.34 Proses Apache HTTP Setelah Penyerangan XerXes.....	4-19
Gambar 4.35 Lalu Lintas Paket Data Setelah Penyerangan XerXes -1.....	4-20
Gambar 4.36 Lalu Lintas Paket Data Setelah Penyerangan XerXes - 2.....	4-20
Gambar 4.37 Perintah Apachekiller	4-21
Gambar 4.38 Proses Penyerangan Apachekiller	4-22
Gambar 4.39 Akses Website Setelah Penyerangan Apachekiller	4-22
Gambar 4.40 Kinerja CPU Setelah Penyerangan Apachekiller	4-23
Gambar 4.41 lalu Lintas Paket Data Setelah Penyerangan Apachekiller -1.....	4-23
Gambar 4.42 lalu Lintas Paket Data Setelah Penyerangan Apachekiller -2.....	4-24
Gambar 4.43 Perintah HULK.....	4-25
Gambar 4.44 Akses Website Setelah Penyerangan HULK.....	4-25
Gambar 4.45 Kinerja CPU Setelah Penyerangan HULK.....	4-26
Gambar 4.46 Lalu Lintas Paket Data Setelah Penyerangan HULK - 1.....	4-26
Gambar 4.47 Lalu Lintas Paket Data Setelah Penyerangan HULK - 2.....	4-27
Gambar 4.48 Hasil Scanning IIS versi 10	4-29
Gambar 4.49 Proses IIS Sebelum Penyerangan.....	4-29
Gambar 4.50 Lalulintas Paket Data Sebelum Penyerangan.....	4-30
Gambar 4.51 Perintah XerXes.....	4-30
Gambar 4.52 Proses Penyerangan XerXes	4-31
Gambar 4.53 Akses Website Setelah Penyerangan XerXes	4-31
Gambar 4.54 Kinerja CPU Setelah Penyerangan XerXes	4-31
Gambar 4.55 Lalu Lintas Paket Data Setelah Penyerangan XerXes.....	4-32



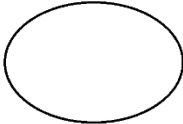
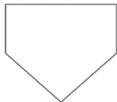
Gambar 4.56 Perintah Apachekiller	4-33
Gambar 4.57 Proses Penyerangan Apachekiller	4-33
Gambar 4.58 Akses Localhost Setelah Penyerangan Apachekiller	4-34
Gambar 4.59 Kinerja CPU Setelah Penyerangan Apachekiller	4-34
Gambar 4.60 lalu Lintas Paket Data Setelah Penyerangan Apachekiller	4-35
Gambar 4.61 Perintah HULK.....	4-36
Gambar 4.62 Akses Website Setelah Penyerangan HULK.....	4-36
Gambar 4.63 Kinerja CPU Setelah Penyerangan HULK.....	4-37
Gambar 4.64 Lalu Lintas Paket Data Setelah Penyerangan HULK.....	4-37
Gambar 4.65 Kinerja CPU Sebelum Penyerangan	4-45
Gambar 4.66 Lalu Lintas Paket Data Sebelum Penyerangan.....	4-45
Gambar 4.67 HoneyBot.....	4-46
Gambar 4.68 Perintah XerXes.....	4-46
Gambar 4.69 Proses Penyerangan XerXes	4-47
Gambar 4.70 Hasil HoneyBot	4-47
Gambar 4.71 Kinerja CPU Setelah Penyerangan.....	4-48
Gambar 4.72 Lalu Lintas Paket Data Setelah Penyerangan	4-48
Gambar 4.73 Akses Localhost Pada Saat Proses Penyerangan Berlangsung	4-49

DAFTAR LAMPIRAN

LAMPIRAN A PENERAPAN WEB SERVER APACHE VERSI 2.2.19	A-1
LAMPIRAN B PENERAPAN WEB SERVER APACHE VERSI 2.4	B-1
LAMPIRAN C PENERAPAN WEB SERVER IIS VERSI 10	C-1
LAMPIRAN D PENERAPAN XERXES.....	D-1
LAMPIRAN E PENERAPAN APACHEKILLER.....	E-1
LAMPIRAN F PENERAPAN HULK.....	F-1
LAMPIRAN G PENERAPAN HONEYBOT	G-1

DAFTAR SIMBOL

Berikut ini merupakan simbol-simbol yang digunakan dalam laporan tugas akhir ini, simbol-simbol tersebut diuraikan pada tabel dibawah ini.

No	Gambar	Nama Gambar	Keterangan
1		<i>Process</i>	Simbol yang digunakan untuk menunjukan aktivitas pengolahan informasi atau menyatakan suatu posisi.
2		Arus/Flow	Simbol yang menyatakan proses dari suatu proses.
3		<i>External Entity</i>	Digunakan untuk menggambarkan apapun atau siapapun yang berinteraksi dengan sistem, baik memberikan informasi kepada sistem ataupun menerima informasi dari sistem.
4		Off-Page Reference	Digunakan untuk menghubungkan symbol-simbol yang berada pada halaman yang berbeda.