



Monitoring Sistem Keamanan Webservice
Simulasi Digital Forensik Dalam Kasus Denial Of Service

TESIS

Oleh
Sri Marini
55410110012

PROGRAM MAGISTER TEKNIK ELEKTRO

PROGRAM PASCA SARJANA

UNIVERSITAS MERCU BUANA

2012



**Monitoring Sistem Keamanan Webserver
Simulasi Digital Forensik Dalam Kasus Denial Of Service**

TESIS

**Diajukan Sebagai Salah Satu Syarat untuk Menyelesaikan Program
Pascasarjana Program Magister Teknik Elektro**

**Oleh
Sri Marini
55410110012**

**UNIVERSITAS MERCU BUANA
PROGRAM PASCA SARJANA**

Pengesahan Tesis

Judul : Monitoring Sistem Keamanan Webserver simulasi Digital Forensik
Dalam Kasus Denial of Service
Nama : Sri Marini
NIM : 55410110012
Program : Pascasarjan Program Magister Teknik Elektro
Konsentrasi : Manajemen Telekomunikasi
Tanggal :

Mengesahkan

Direktur Pascasarjana :



Prof. Dr. Didik J. Rachbini

Ketua program studi

Magister Teknik Elektro



Dr.-Ing Mudrik Alaydrus

Pembimbing I



Dr.-Ing Mudrik Alaydrus

Pembimbing II



Rizal Bahaweres, Mkom

iii



UNIVERSITAS
MERCU BUANA



UNIVERSITAS
MERCU BUANA

Pernyataan

Saya yang bertanda tangan dibawah ini menyatakan dengan sebenar-benarnya bahwa seluruh tulisan dan pernyataan dalam tesis ini :

Judul : monitoring Sistem Keamanan Webserver simulasi Digital Forensik
Dalam Kasus Denial of Service

Nama : Sri Marini

NIM : 55410110012

Program : Pascasarjan Program Magister Teknik Elektro

Konsentrasi : Manajemen Telekomunikasi

Tanggal :

Merupakan hasil studi pustaka, penelitian lapangan, dan karya saya sendiri dengan bimbingan Pembimbing yang ditetapkan dengan surat keputusan Ketua Program studi Magister Teknik Elektro Universitas Mercu Buana.

Tesis ini belum pernah diajukan untuk memperoleh gelar magister pada program sejenis diperguruan tinggi lain Semua informasi, data, dan hasil pengolahannya yang digunakan, Telah dinyatakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

Jakarta,


Sri Marini



iv

UNIVERSITAS
MERCU BUANA



UNIVERSITAS
MERCU BUANA

Kata Pengantar

Puji dan syukur saya panjatkan kepada Allah SWT yang telah melimpahkan karunia dan rahmatNYA sehingga saya dapat menyelesaikan penulisan tesis ini, dengan judul “ Monitoring Sistem Keamanan Webservice simulasi Digital Forensik Dalam Kasus Denial of Service”

Tesis ini disusun dan diajukan untuk memenuhi sebagian persyaratan dalam penyelesaian jenjang Studi Strata-2 di Universitas Mercu Buana, Jakarta dalam rangka memperoleh gelar kesarjanaan Magister Teknik (MT) Program Magister Teknik Elektro. Tesis ini merupakan Latar Belakang masalah atau tema topic penulis pilih serta landasan teori yang berhubungan dengan Monitoring Sistem Keamanan Webservice simulasi Digital Forensik Dalam Kasus Denial of Service

Selama penulisan Tesis, Penulis banyak dibantu dan didukung moral dari berbagai pihak. Oleh karena itu penulis menyampaikan terima kasih yang setulusnya kepada:

Kedua orang tua saya Bpk Kgs.M.Toha munir dan Ibu.Siti Rohana yang telah sukses membesarkan dan menjadikan anak-anaknya tumbuh dan berkembang menjadi anak yang soleh dan soleha berguna bagi Negara dan bangsa.

Suami saya Bpk.Habib Muhammadin al-atas yang telah memberikan dukungan moril dan spiritual, semangat, dan selalu mengingatkan penulis dalam menyelesaikan tugas akhir ini. Gelar S2 ini saya persembahkan kepada suami saya yang telah berjasa hingga saya menjadi seperti sekarang ini.

Bapak Rizal Broer Bahaweres, M.Kom selaku Dosen Pembimbing Tesis saya yang telah membantu dalam memberikan arahan dan masukan yang sangat berharga dan bermanfaat dalam penulisan Tesis ini dari awal hingga selesai.

Bapak Dr._Ing.Mudrik Alaydrus selaku Ketua Program Studi Magister Teknik Elektro dan Dosen Pembimbing yang telah membantu dalam memberikan arahan dan masukan yang sangat berharga dan bermanfaat dalam penulisan Tesis ini sehingga penulis menyelesaikan Tesis ini.

Teman-teman di Program Studi MTEL khususnya angkatan 7, Terima kasih atas dukungannya sehingga tesis ini dapat diselesaikan.

Rektor, Dekan, Para Dosen dan seluruh Staff Tata Usaha Program Pasca Sarjana Universitas Mercu Buana, Terima kasih sudah membangkitkan semangat penulis untuk selalu berusaha dalam menyelesaikan Tesis ini.

Kakak dan adik saya yang telah membantu dan memberikan support kepada penulis.

Saya menyadari bahwa penulisan Tesis ini masih banyak kekurangan-kekurangan sehingga dibutuhkan saran dan kritik yang membangun untuk penyempurnaan penelitian di masa yang akan datang. Dan akhir kata Penulis berharap semoga Tesis ini dapat bermanfaat bagi pembacanya.

UNIVERSITAS
MERCU BUANA

Jakarta,

Daftar Isi

JUDUL LUAR.....	i
JUDUL DALAM	ii
Pengesahan Tesis	iii
Pernyataan	iv
Kata Pengantar.....	v
Abstrak	vii
Abstract	viii
Daftar Isi.....	ix
Daftar Gambar	xii
Daftar Tabel.....	xiii
Daftar Istilah.....	xiv
BAB 1 Pendahuluan.....	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	5
1.3 Batasan Penelitian.....	5
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian.....	6
1.6 Metode Penelitian	6
1.7 Sistematika Penulisan	7
BAB 2 Kajian Pustaka	10
2.1 Penelitian Terkait.....	10

2.1.1	Tujuan Digital Forensik	11
2.1.2	Barang Bukti Digital Sebagai Alat Bukti Sah.....	12
2.1.3	Web Server.....	12
2.2	Denial of Service	21
2.2.1	Tipe Serangan Dos/DDoS.....	22
2.2.2	Efek Dari Serangan Dos.....	23
2.2.3	Jenis-jenis Serangan Dos	24
2.3	Serangan DoS dengan Slowloris	25
2.4	Undang – Undang ITE.....	25
2.4.1	Skenario Kajian UU ITE Kasus Cybercrime	27
2.5	Sejarah Backtrack	30
BAB 3	Metodologi Penelitian	33
3.1	Studi Literatur.....	34
3.2	Simulasi Proses Forensik	35
3.3	Skenario Pengujian	36
3.3.1	Analisa Use case Serangan DoS dengan Slowloris Attacker....	36
3.3.2	Skenario Simulasi Penyerangan	37
3.3.3	Skenario Pengujian server menggunakan slowloris pd backtrack	39
BAB 4	Hasil dan Pembahasan.....	40
4.1	Implementasi Analisa Penelitian	40
4.2	Pengambilan Data dari Test Bed	64
4.3	Simulasi Penyerangan.....	65
4.4	pembahasan	56

BAB 5	Kesimpulan dan Saran.....	66
5.1	Kesimpulan	66
5.2	Saran	66
	Daftar Pustaka.....	67
	Lampiran	69



Daftar Gambar

Gambar I.1 Pengguna Internet diindonesia tahun 2000-2010.....	1
Gambar 1.2 Penetrasi Pengguna Internet diindonesia tahun 2010-2011	2
Gambar I.3 Pengguna Internet didunia tahun 2010	3
Gambar I.4 menggambarkan char serangan Web 2009	4
Gambar 2.1 Penggambaran Penelitian Terkait dengan Penelitian ini	10
Gambar 2.2 classification of the denial of service attacks.....	21
Gambar 2.3 DoS Attack	22
Gambar 2.4 Kajian Undang-Undang ITE terhadap serangan DOS	27
Gambar 3.1 Metodologi penelitian pada penelitian ini.....	33
Gambar 3.2 Ilustrasi metodologi penelitian secara umum	34
Gambar 3.3 proses digital forensik	35
Gambar 3.4 lifecycle serangan	35
Gambar 3.5 Skenario pengujian	36
Gambar 3.6 Use case Serangan DoS dengan Slowloris.....	36
Gambar 3.7 Simulasi Penyerangan.....	37
Gambar 3.8 Aktivitas diagram mencari kelemahan system web	38
Gambar 3.9 Skenario Pengujian server menggunakan slowloris pada backtrack.	39
Gambar 4.1 Tampilan Script Lbd.sh.....	55
Gambar 4.2 Tampilan script slowloris.pl.....	55
Gambar 4.3 Tampilan menyimpan script lbd.sh pada desktop	55
Gambar 4.4 Tampilan kode script lbd.....	56
Gambar 4.5 Tampilan lbd.sh untuk pengecekan load balancing.....	56
Gambar 4.6 Tampilan menyimpan file slowloris pada destop.....	57
Gambar 4.7 Tampilan script slowloris.pl.....	57
Gambar 4.8 Tampilan penyimpanan script slowloris.pl	58
Gambar 4.9 Tampilan script lbd dijalankan	58

Gambar 4.10 Tampilan output pengetesan script lbd.....	58
Gambar 4.11 Tampilan melakukan pengecekan auto balancing pada target	58
Gambar 4.12 Tampilan pada saat ngeping target	59
Gambar 4.13 Tampilan output ping target	59
Gambar 4.14 Tampilan IP target	59
Gambar 4.15 Tampilan proses checking for http	60
Gambar 4.16 Tampilan checking for http	60
Gambar 4.17 Tampilan output checking for http	61
Gambar 4.18 Tampilan script slowloris.pl.....	61
Gambar 4.19 Tampilan nge-ping web target.....	62
Gambar 4.20 Tampilan penyerangan target	62
Gambar 4.21 Tampilan serangan slowloris mengetahui limit timeout	63
Gambar 4.22 Tampilan TCP connection timeout.....	63
Gambar 4.23 Tampilan Kondisi computer target	64
Gambar 4.24 Tampilan kondisi Target the connection time out.....	64

UNIVERSITAS
Daftar Tabel
MERCU BUANA

Tabel 2.1 kejahatan cybercrime yang terjadi di Indonesia dan diluar negeri.....	28
Tabel 4.2 Hasil Tangkapan komunikasi yang terjadi menggunakan backtrack	65

Daftar Istilah

- * -dns : the target (dapat berupa IP atau domain)
- * -port : port yg di gunakan oleh webservice (80)
- * -timeout: nilai waktu delay timeout untuk setiap paket thread, penantian reacquiring ruang tcp di server. pada langkah pengetesan, Nilai ini diisi dengan flag -test
- * -num : jumlah socket yang digunakan untuk mendapatkan koneksi. Biasanya server apache akan membutuhkan nilai antara 400-600 atau tergantung pada konfigurasi
- * -tcpto : TCP Timeout.
- * -httpready: HTTPReady di gunakan apache untuk buffer connections. attacker dapat melewati perlindungan ini dengan mengirimkan permintaan POST bukan GET atau HEAD.

