

SKRIPSI

**PRARANCANGAN SISTEM PENDETEKSI PENYUSUP (INTRUSION
DETECTION SYSTEM) DENGAN VIRTUAL HOST PADA SERVER**

Diajukan guna melengkapi sebagian syarat
Dalam mencapai gelar sarjana Strata Satu (S1)

Disusun oleh:

Nama : Susilo Widakdo

NPM : 2004225007



**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS BHAYANGKARA JAKARTA RAYA**

2009

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini,

Nama : Susilo Widakdo
NPM : 2004225007
Jurusan : Teknik Informatika
Judul tugas akhir : Perancangan Sistem Pendeteksi Penyusup
(Intrusion Detection System) Dengan Virtual Host
Pada Server

Dengan ini menyatakan bahwa hasil penulisan skripsi yang telah saya buat ini merupakan hasil karya sendiri dan benar keasliannya. Apabila ternyata di kemudian hari penulisan skripsi ini merupakan hasil plagiat atau penjiplakan terhadap karya orang lain, maka saya bersedia mempertanggungjawabkan sekaligus bersedia menerima sanksi berdasarkan aturan tata tertib di Universitas Bhayangkara Jakarta Raya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Penulis

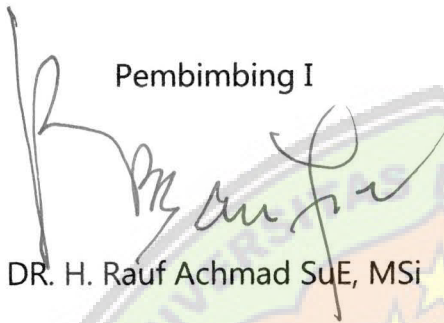
(Susilo Widakdo)

LEMBAR PENGESAHAN

**PERANCANGAN SISTEM PENDETEKSI PENYUSUP
(INTRUSION DETECTION SYSTEM)
DENGAN VIRTUAL HOST PADA SERVER**

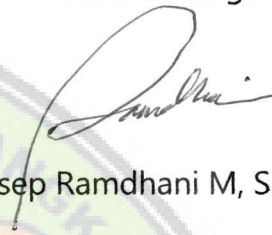
Menyetujui,

Pembimbing I



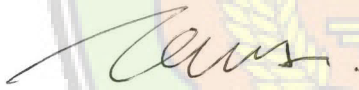
DR. H. Rauf Achmad SuE, MSi

Pembimbing II



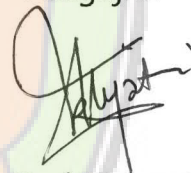
Asep Ramdhani M, SKomp

Penguji I



Hendarman, M.Kom

Penguji II



Ir. Ruci Meiyanti

Mengetahui,



Ketua Jurusan Teknik Informatika
Universitas Bhayangkara Jakarta Raya



Ismaniah, SSi, MM

ABSTRAKSI

SUSILO WIDAKDO, 2004225007, PRARANCANGAN SISTEM PENDETEKSI PENYUSUP (INTRUSION DETECTION SYSTEM) DENGAN MENGGUNAKAN VIRTUAL HOST PADA SEVER.

Intrusion detection system (IDS) adalah teknik dan metode yang digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah jaringan dan *host level*. *Intrusion detection system* terbagi dalam dua kategori dasar: *signature-based detection systems* dan *anomaly detection system*, seorang *intruder* mempunyai jejak, seperti *virus* komputer, yang dapat terdeteksi dengan menggunakan *software*. Dengan menggunakan pendeteksi jejak dan aturan-aturan, sistem pendeteksi dapat menemukan dan mencatat aktivitas yang mencurigakan dan memberikan sebuah peringatan akan adanya bahaya, usaha pendeteksi *intruder* biasanya tergantung pada besaran paket data yang terdapat pada *header protocol*. Dalam beberapa kasus metode ini lebih baik dibandingkan dengan *signature-based IDS*, biasanya sebuah *intrusion detection system* menangkap paket data yang mencurigakan dari jaringan dan melaporkan dalam sebuah informasi atas aktivitas yang mencurigakan di dalamnya.

Dengan adanya *intrusion detection system* dengan menggunakan *virtual host* akan membuat pertahanan sebuah *server* menjadi semakin kuat, selain itu, proses pengidentifikasian akan aktivitas yang mencurigakan akan lebih mudah, karena usaha yang dilakukan oleh *intruder* dalam menembus pertahanan sebuah *server* tidak secara langsung, melainkan kepada sebuah *virtual server* yang terdapat didalam *server* tersebut.



KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah S.W.T, karena Rahmat-Nya penulis dapat menyelesaikan karya ilmiah ini. Adapun maksud penyusunan karya ilmiah ini adalah untuk memenuhi salah satu persyaratan dalam menempuh pendidikan tinggi jenjang strata satu (S1) pada Fakultas Teknik Universitas Bhayangkara Jakarta Raya, karya ilmiah ini berjudul "Perancangan Sistem Pendeteksi Penyusup (*Intrusion Detection System*) Dengan Menggunakan *Virtual Host* Pada *Server*."

Sekilas menyinggung isi dari karya ilmiah ini adalah mengenai perancangan sebuah sistem pendeteksi penyusup (*intrusion detection system*) dengan menggunakan *virtual host* di dalam sebuah *server*, selain itu pembahasan yang akan dibahas terdapat beberapa poin penting di dalamnya mengenai cara menggunakan sistem penyusup, mengidentifikasi adanya aktifitas-aktifitas yang mencurigakan, penyesuaian sistem pendeteksi penyusup dengan komputer *server* dan sedikit contoh penerapan sistem pendeteksi penyusup dengan menggunakan *virtual host*.

Banyak kesulitan dan hambatan yang dialami oleh penulis dalam menyusun karya ilmiah ini terutama dalam mendapatkan bahan materi dan mengolahnya, tetapi semua itu telah dapat diatasi dengan baik berkat

dukungan dan bantuan dari berbagai pihak. Untuk itulah pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Bapak Irjen Pol. (Purn) Drs. Logan Siagian, MH, selaku Rektor Universitas Bhayangkara Jakarta Raya.
2. Bapak DR. H. Rauf Achmad Sue, MSi, selaku Dekan Fakultas Teknik Universitas Bhayangkara Jakarta Raya.
3. Ibu Ismaniah, SSi, MM, selaku Ketua Jurusan Teknik Informatika Universitas Bhayangkara Jakarta Raya.
4. Bapak Asep Ramdhani M., ST, selaku pembimbing dua dari karya ilmiah ini.
5. Dan terakhir kepada teman-teman FT dan pihak-pihak yang tidak dapat saya sebutkan satu-persatu tanpa mengurangi rasa hormat penulis.

Semoga dengan adanya karya ilmiah ini dapat menjelaskan gambaran umum tentang perancangan dan penerapan sistem pendeteksi penyusup pada sebuah server dengan menggunakan *virtual host*, akhir kata, semoga karya ilmiah ini dapat bermanfaat bagi kita semua.

Bekasi, Maret 2009

Penulis

DAFTAR ISI

Halaman Judul	i
Halaman Pernyataan	ii
Halaman Pengesahan	iii
Abstraksi	iv
Kata Pengantar	vi
Daftar Isi	viii
Daftar Tabel	xii
Daftar Gambar	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	5
1.3 Batasan Masalah	5
1.4 Maksud dan Tujuan	6
1.2.1 Maksud	6
1.2.2 Tujuan	6
1.5 Metode Penelitian	7
1.5.1 Metode Observasi	8
1.5.2 Studi Pustaka	9
1.5.3 Eksperimen	9
1.6 Sistematika Penulisan	10
BAB II TINJAUAN PUSTAKA	13
2.1 Pengertian Perancangan	12
2.2 Sistem Pendeteksi Penyusup	14
2.3 Virtual Host	15
2.4 Jaringan Komputer	16

2.5	Lokal Area Network (LAN)	16
2.6	Metropolitan Area Network (MAN)	17
2.7	Wide Area Network (WAN)	17
2.8	Asymmetric Digital Subscriber Lines (ADSL)	17
2.9	Bandwidth	18
2.10	Ping	18
2.11	Topologi Jaringan Komputer	19
2.11.1	Topologi Bus	19
2.11.2	Topologi Token Ring	19
2.11.3	Topologi Star	19
2.12	Linux	20
2.13	Gateway	22
2.14	Router	22
2.15	Server	23
2.16	Internet	24
2.17	User Datagram Protocol (UDP)	26
2.18	Internet Control Message Protocol (ICMP)	27
2.19	Transmission Control Protocol/Internet Protocol (TCP/IP)	27
2.20	Common Intrusion Detection Framework (CIDF)	29
2.21	Common Intrusion Specification Language (CISL)	29

BAB III PERANCANGAN SISTEM PENDETEKSI PENYUSUP (INTRUSION DETECTION SYSTEM) DENGAN MENGGUNAKAN VIRTUAL HOST PADA SERVER	30
3.1 Perancangan Server	31
3.1.1 Spesifikasi Perangkat Keras	32
3.1.2 Proses Penginstalan Sistem Operasi	32
3.2 Evaluasi Perancangan Server	40

3.3	Proses Penginstalan Virtual Host	41
3.4	Evaluasi Penginstalan Virtual Host	44
3.5	Konfigurasi Virtual Host	45
3.6	Evaluasi Konfigurasi Virtual Host	45
BAB IV	HASIL DAN PEMBAHASAN	47
4.1	Alur Hidup Sistem Pendeteksi Penyusup	47
4.2	Keuntungan Honeypot	50
4.3	Kerugian Honeypot	51
4.4	Kategori Sistem Pendeteksi Penyusup	52
4.4.1	Application IDS	52
4.4.2	File Integrity Checkers	53
4.4.3	Host Based IDS	53
4.4.4	Hybrid IDS	54
4.4.5	Network IDS (NIDS)	54
4.4.6	Personal Firewall	55
4.4.7	Targeted-based IDS	56
4.4.8	Network Intrusion Prevention System / Inline IDS	56
4.4.9	Host Intrusion Prevention System	56
4.4.10	DDOS Mitigating Tool	57
4.5	Pengidentifikasian Sistem Operasi Berdasarkan Time To Life	57
4.6	Pengidentifikasian Aktifitas-aktifitas Yang Mencurigakan Pada Server	60
4.7	Contoh Penerapan Virtual Host Pada Server	62
4.8	Contoh Teknik Serangan Peretas	65
4.8.1	Deskripsi Ping of Death	66
4.8.2	Deskripsi Protokol	66
4.8.3	Catatan Dari Proses Serangan	69

4.8.4 Perintah Ping of Death	69
4.8.5 Cara Mengatasi Serangan	70
4.9 Perbandingan Sistem Pendeteksi Penyusup	71
BAB V KESIMPULAN DAN SARAN	72
5.1 Kesimpulan	72
5.2 Saran	74
DAFTAR PUSTAKA	75
LAMPIRAN	77



DAFTAR TABEL

Tabel 1.1 Tabel Penelitian	7
Tabel 4.1 Tabel Time To Life (TTL)	58



DAFTAR GAMBAR

Gambar 2.1 Topologi Bus	19
Gambar 2.2 Topologi Token Ring	19
Gambar 2.3 Topologi Star	20
Gambar 3.1 Pemilihan Bahasa	33
Gambar 3.2 Pemilihan Proses Pengistalan	33
Gambar 3.3 Proses Identifikasi Perangkat Keras	34
Gambar 3.4 Pemilihan Bahasa Sistem Operasi	34
Gambar 3.5 Pemilihan Waktu	35
Gambar 3.6 Pemilihan Tampilan Keyboard	35
Gambar 3.7 Pemilihan Hard disk	36
Gambar 3.8 Pengisian Profil Pengguna	36
Gambar 3.9 Informasi Pengaturan Sistem Operasi	37
Gambar 3.10 Pemilihan Bootloader	37
Gambar 3.11 Proses Instalasi	38
Gambar 3.12 Instalasi Selesai	38
Gambar 3.13 Proses Restart	39
Gambar 3.14 Proses Login	39
Gambar 3.15 Tampilan Desktop Ubuntu 8.10	40
Gambar 4.1 Sistem Pendeteksi Penyusup	48
Gambar 4.2 Arsitektur Honeyd	49
Gambar 4.3 Proses Ping	63
Gambar 4.4 Skema Denial of Service	65