

**ANALISIS DAN PENGEMBANGAN SISTEM DETEKSI PENYUSUP
DALAM JARINGAN PEER TO PEER
DENGAN OS LINUX**

SKRIPSI



disusun oleh

Budi Tiar Saputra

07.11.1824

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2011**

**ANALISIS DAN PENGEMBANGAN SISTEM DETEKSI PENYUSUP
DALAM JARINGAN PEER TO PEER
DENGAN OS LINUX**

Skripsi

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Budi Tiar Saputra

07.11.1824



**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2011**

PERSETUJUAN

SKRIPSI

**Analisis Dan Pengembangan Sistem Deteksi Penyusup
Dalam Jaringan Peer To Peer Dengan OS Linux**

yang dipersiapkan dan disusun oleh

Budi Tiar Saputra

07.11.1824

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 05 April 2011

Dosen Pembimbing,


Melwin Syafrizal, S.Kom., M.Eng
NIK. 190302105

PENGESAHAN

SKRIPSI

Analisis dan Pengembangan Sistem Deteksi Penyusupan Sederhana Dalam Jaringan Peer To Peer Dengan OS Linux

yang dipersiapkan dan disusun oleh

Budi Tiar Saputra

07.11.1824

telah dipertahankan di depan Dewan Penguji
pada tanggal 04 Juni 2011

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Kusnawi, S.Kom, M. Eng.
NIK. 190302112



Erik Hadi Saputra, S.Kom, M.Eng.
NIK. 190302107



Melwin Syafrizal, S.Kom., M.Eng.
NIK. 190302105



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 4 Juni 2011

KETUA STMIK AMIKOM YOGYAKARTA



Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 8 Juni 2011



Budi Tiar Saputra

07.11.1824

MOTTO

"ga da yang ga mungkin"

(anja)

*"relakanlah diri kita untuk melakukan yang terbaik kepada orang disekitar kita,,
lalu lihatlah apa yang terjadi"*

(Mario Teguh)

"ikhilaskan diri, yakin kalau semuanya itu rencana yang sempurna dari Allah"

(mama)

"do it by Watch, Learn, Analyze, Think, then Do"

(biohazzard)

"selesaikan segalanya itu sekarang"

(btx)

*"Be extremely subtle, even to the point of formlessness. Be extremely mysterious,
even to the point of soundlessness. Thereby you can be the director of the
opponent's fate"*

(Sun Tzu)

PERSEMBAHAN

Skripsi ini kupersembahkan untuk :

- ◆ **Mama, mama, dan MAMA**
...ma...tra dah lulus (walaupun telat)..moga tra dah sedikit bisa nyenengin mama yaa..
- ◆ **Papa, Kakak-kakak, Abang-abang, dan adikku**
Makasih atas semua dukungannya
- ◆ **HMJTI STMIK AMIKOM Yogyakarta**
Salam hormat pada seluruh pengurus, mantan pengurus, serta kader HMJTI yang telah membimbing saya dalam berorganisasi di STMIK Amikom Yogyakarta, unggul dalam tren teknologi informasi tapi belum tren dalam organisasi
- ◆ **FOSSIL STMIK AMIKOM Yogyakarta**
Be free, be open source !
- ◆ **Ryan (Fajriana Nugraha), Andri (Bambang Andrie Gunawan), Ojan (Sandy Fauzan), Rista (Nurista Anggaeni), Ali (Ali Mahfud), Putri (Putri Riyanti)**
Kalian bener-bener bikin aku bangga jadi teman kalian, luv u all guys!
- ◆ **Adi Pujiono, Faizal Akbar, Tian Wahyutomo, Rully Ardiato, I Made Deni, dan anak-anak HMJTI, FOSSIL, dan ONEGAI lainnya**
Lanjutkan perjuangan...ingat teman, organisasi mengajarkan kita segalanya!!
- ◆ serta semua orang yang telah banyak memberikan dukungan, bantuan dalam bentuk apapun hingga terselesaikannya skripsi ini tapi belum tersebut namanya

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah SWT yang hanya dengan rahmat dan hidayahnya, penulis mampu menyelesaikan skripsi dengan judul “ANALISIS DAN PENGEMBANGAN SISTEM DETEKSI PENYUSUP DALAM JARINGAN PEER TO PEER DENGAN OS LINUX” ini dapat terselesaikan. Serta shalawat dan salam kepada junjungan penulis, Muhammad SAW.

Skripsi ini dibuat untuk memenuhi salah satu syarat untuk memperoleh gelar sarjana Strata 1 (S1), jurusan Teknik Informatika di STMIK Amikom Yogyakarta. Banyak pihak yang telah membantu hingga skripsi ini terselesaikan. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih sebesar-besarnya kepada:

- Bapak Melwin Syafrizal, S. Kom, M.Eng, selaku dosen pembimbing
- Bapak Sudarmawan, MT, selaku Ketua Jurusan D3-Teknik Informatika
- Bapak Abas Ali Pangera, Ir, M. Kom selaku Ketua Jurusan S1-Teknik Informatika
- Mandriva Community, teman-teman dunia maya yang sangat membantu
- dan pihak-pihak lain yang tidak mungkin disebutkan satu persatu

Penulis yakin, skripsi ini masih jauh dari kesempurnaan, oleh karena itu penulis memohon kritik dan saran yang membangun untuk skripsi ini. Hingga demikian skripsi akan dapat lebih berguna bagi siapapun pembaca skripsi ini.

Yogyakarta, Juni 2011

Penulis

DAFTAR ISI



HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
LEMBAR PENGESAHAN.....	iii
LEMBAR PERNYATAAN.....	iv
MOTTO.....	v
PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
INTISARI.....	xiii
ABSTRACT.....	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Metode Pengumpulan Data.....	3
1.6.1 Eksperimen.....	3
1.6.2 Observasi.....	4
1.6.3 Sumber bacaan/Pustaka.....	4
1.7 Sistematika Penulisan.....	4
BAB II LANDASAN TEORI.....	6
2.1 Tinjauan Pustaka.....	6
2.2 Keamanan Jaringan.....	7
2.3 Firewall dan Sistem Deteksi Penyusupan.....	7
2.3.1 Firewall	7
2.3.2 Sistem Deteksi Penyusupan.....	8

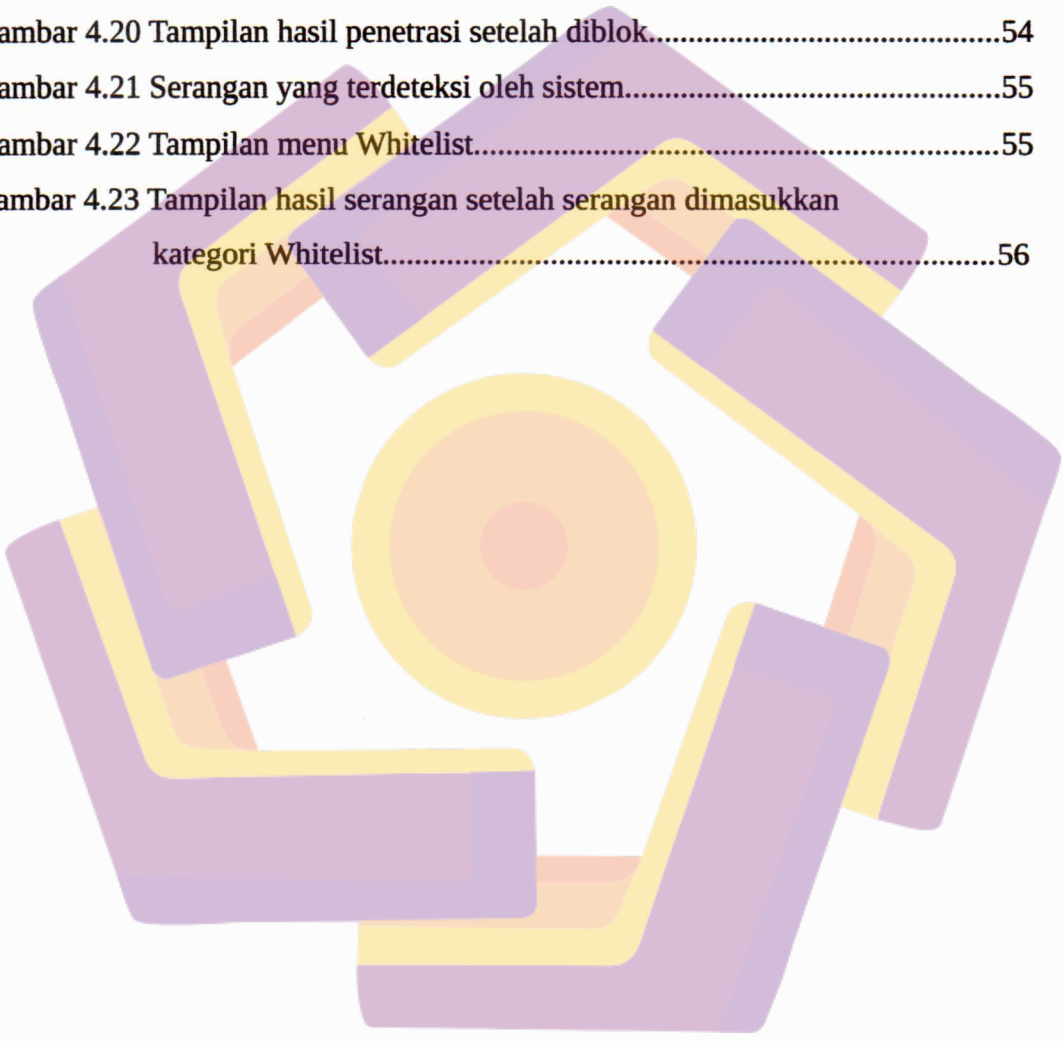
2.3.3 Perbedaan Firewall dan Sistem Deteksi Penyusupan.....	10
2.4 Metode Serangan/Penetrasi dari Penyusup.....	10
2.4.1 Identifikasi Port (Port Identification).....	11
2.4.2 Spoofing.....	11
2.4.3 Priviledge scalation.....	12
2.5 Karakter dari Tiap Serangan.....	13
2.5.1 Port mapping.....	13
2.5.2 Network Identification.....	13
2.5.3 Protocol manipulation.....	13
2.5.4 Vulnerability escalation.....	13
2.6 Software Penetrasi dan Monitoring Jaringan.....	14
2.6.1 Nmap.....	14
2.6.2 TuxCut.....	15
2.6.3 AngryIPScanner.....	15
2.6.4 EtterCap.....	16
BAB III ANALISIS DAN PERANCANGAN SISTEM.....	18
3.1 Perancangan Sistem.....	18
3.2 Bentuk antar muka sistem.....	18
3.2.1 Tampilan utama.....	19
3.2.2 Tampilan bila terjadi serangan.....	19
3.2.3 Tampilan kategori whitelist.....	20
3.2.4 Tampilan kategori blacklist.....	20
3.3 Analisis Kebutuhan.....	21
3.3.1 Kebutuhan Perangkat Keras (Hardware).....	21
3.3.2 Kebutuhan Perangkat Lunak (Software).....	22
3.4 Analisis Sistem.....	25
3.4.1 Sistem yang berjalan sekarang.....	25
3.4.2 Sistem yang direncanakan.....	25
BAB IV IMPLEMENTASI DAN PEMBAHASAN.....	27
4.1 Instalasi Software.....	27

4.2 Pembangunan Sistem.....	27
4.2.1 Sistem Pendeteksi Penyusupan.....	27
4.2.2 Sistem Pemberi Alert.....	38
4.3 Analisis Implementasi Sistem.....	44
4.3.1 Uji implementasi sistem.....	44
4.3.2 Uji identifikasi serangan.....	45
4.3.3 Uji pemanfaatan menu blacklist dan whitelist.....	52
4.4 Konfigurasi dan Implementasi Sistem.....	56
4.4.1 Konfigurasi Sistem pada Mandriva 2010.2 (Henry_Farman).....	56
4.4.2 Implementasi Sistem.....	58
BAB V PENUTUP.....	60
5.1 Kesimpulan.....	60
5.2 Saran.....	61
DAFTAR PUSTAKA	
LAMPIRAN	

DAFTAR GAMBAR

Gambar 2.1 Skema pengamanan dengan firewall.....	8
Gambar 2.2 Skema pemanfaatan IDS dalam sebuah jaringan.....	8
Gambar 2.3 Tampilan Nmap.....	14
Gambar 2.4 Tampilan TuxCut.....	15
Gambar 2.5 Bentuk tampilan AngryIPScanner.....	15
Gambar 2.6 Bentuk tampilan Ettercap.....	16
Gambar 3.1 Diagram alir sistem deteksi penyusupan.....	18
Gambar 3.2 Rancangan tampilan utama.....	19
Gambar 3.3 Rancangan tampilan alert.....	19
Gambar 3.4 Rancangan tampilan kategori Whitelist.....	20
Gambar 3.5 Rancangan tampilan kategori Whitelist.....	30
Gambar 3.6 Bentuk tampilan Drakfirewall.....	24
Gambar 3.7 Skema rancangan sistem pada client.....	26
Gambar 4.1 Tampilan kompilasi sistem melalui terminal.....	37
Gambar 4.2 Tampilan utama sistem yang dibangun.....	44
Gambar 4.3 Tampilan tab Blacklist.....	44
Gambar 4.4 Tampilan tab Whitelist.....	45
Gambar 4.5 Penetrasi menggunakan AngryIPScanner.....	45
Gambar 4.6 Melakukan penetrasi menggunakan fasilitas open trace pada AngryIPScanner.....	46
Gambar 4.7 Tampilan report penetrasi dengan AngryIPScanner.....	46
Gambar 4.8 Tampilan sistem ketika penyusup terdeteksi.....	47
Gambar 4.9 Tampilan sistem ketika penyerangan terdeteksi.....	47
Gambar 4.10 Tampilan penyerangan menggunakan Nmap.....	48
Gambar 4.11 Tampilan notifikasi terjadinya serangan.....	49
Gambar 4.12 Tampilan sistem ketika mendeteksi serangan dari Nmap.....	49
Gambar 4.13 Tampilan penyerangan menggunakan TuxCut.....	50
Gambar 4.14 Tampilan browser pada komputer target setelah	

di serang dengan Tuxcut.....	51
Gambar 4.15 Tampilan penetrasi menggunakan Ettercap.....	51
Gambar 4.16 Tampilan browser komputer target ketika diserang menggunakan Ettercap.....	52
Gambar 4.17 Tampilan serangan menggunakan Nmap.....	53
Gambar 4.18 Serangan terdeteksi oleh sistem.....	53
Gambar 4.19 Serangan dikategorikan sebagai blacklist.....	54
Gambar 4.20 Tampilan hasil penetrasi setelah diblok.....	54
Gambar 4.21 Serangan yang terdeteksi oleh sistem.....	55
Gambar 4.22 Tampilan menu Whitelist.....	55
Gambar 4.23 Tampilan hasil serangan setelah serangan dimasukkan kategori Whitelist.....	56



INTISARI

Penggunaan jaringan komputer dewasa ini telah begitu meluas. Hal ini dikarenakan penggunaan internet dan komputer di jaringan sudah menjadi kebutuhan. Namun amat disayangkan bila keamanan komputer yang menggunakan jaringan tersebut (*client*) tidak ikut berkembang bersamaan dengan giatnya pertumbuhan jaringan komputer. Komputer ini, membutuhkan sistem pengamanan tambahan yang mampu memberi jaminan kenyamanan dalam menggunakan fasilitas jaringan internet saat sistem operasi digunakan.

Penelitian dilakukan dengan melakukan eksperimen, yaitu mulai dari instalasi sistem operasi Mandriva 2010.2 (Henry_Farman) sebagai sistem operasi tempat sistem akan dibangun, integrasi dan instalasi sistem yang dirancang, hingga pengujian penetrasi sistem deteksi penyusupan yang telah dibangun pada sistem operasi dengan *software-software* yang biasa digunakan untuk melakukan penetrasi dalam jaringan. Hasil pengujian penetrasi ini didokumentasikan, sehingga dapat memberikan gambaran kemampuan sistem ini nantinya.

Hasil dari penelitian ini menyimpulkan bahwa firewall dapat digunakan sebagai pendeteksi penyusupan, namun sistem ini hanya mampu mendeteksi serangan yang berpola *echo request* saja. Untuk mengintegrasikan sistem ini pada sistem operasi Mandriva 2010.2 (Henry_Farman), dibutuhkan konfigurasi tambahan, yaitu berupa *installer*.

Kata kunci: keamanan, pengguna jaringan komputer, aplikasi pengaman, linux, deteksi penyusup

ABSTRACT

Implementation of networked computer this time has been so widely. This is because the internet using and computer on a network has become a needs. But it is so unfortunately if the security of computer on that network (the client) was not growth as rapidly the growth of computer network. This computer, require additional security system that is guarantees of the comfort to using the internet network facility when the operating system used.

This research carried out by conducting experiments, ie starting from the operating system installation Mandriva 2010.2 (Henry_Farman) as an operating system where the system will be built, integration and installation of systems that are designed, then penetration testing intrusion detection systems that have been built in the operating system with software that used to penetrating the network. The results of penetration testing is documented, so as to give an idea of this system capabilities later.

The results of this study concluded that a firewall can be used as intrusion detection, but this system is only able to detect a pattern of attacks echo request only. To integrate this system on the operating system Mandriva 2010.2 (Henry_Farman), an additional configuration is needed, such as the installer configuration.

Keywords: security, network computers client, security application, linux, intruder detection

