

**IMPLEMENTASI SISTEM DETEKSI PENYUSUPAN
PADA JARINGAN KOMPUTER**

SKRIPSI



Oleh :

YUDHI ARDIYANTO

2000120068

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH YOGYAKARTA

2008

**IMPLEMENTASI SISTEM DETEKSI PENYUSUPAN
PADA JARINGAN KOMPUTER**

Diajukan sebagai salah satu syarat memperoleh gelar Sarjana Teknik program S-1
pada Jurusan Teknik Elektro, Fakultas Teknik, Universitas Muhammadiyah

Yogyakarta

SKRIPSI



Oleh :

YUDHI ARDIYANTO

2000120068

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH YOGYAKARTA

2008

HALAMAN PERNYATAAN

Semua yang tertulis dalam naskah skripsi ini adalah benar-benar merupakan hasil karya saya sendiri dan atau bukan menjiplak hasil karya orang lain. Apabila di kemudian hari terbukti pernyataan ini tidak benar, maka saya siap menerima sanksi dari Universitas Muhammadiyah Yogyakarta sesuai dengan peraturan yang berlaku.

Yogyakarta, 3 November 2008

Yang menyatakan,



Yudhi Ardiyanto

HALAMAN PENGESAHAN I

SKRIPSI

IMPLEMENTASI SISTEM DETEKSI PENYUSUPAN

PADA JARINGAN KOMPUTER



Dosen Pembimbing Utama

Dosen Pembimbing Muda

HALAMAN PENGESAHAN II

SKRIPSI

IMPLEMENTASI SISTEM DETEKSI PENYUSUPAN PADA JARINGAN KOMPUTER

Skripsi ini telah dipertahankan dan disahkan di depan dewan penguji pada tanggal
3 November 2008.

Dewan Penguji :

1. Ir. Dwijoko Purbohadi, MT
(Ketua penguji / Pembimbing utama)
2. M. Helmi Zain Nuri, ST, MT
(Penguji anggota / Pembimbing muda)
3. Helman Muhammad, ST, MT
(Penguji anggota)
4. Haris Setyawan, ST
(Penguji anggota)

Menyetujui,

Ketua Jurusan

Teknik Elektro Universitas Muhammadiyah Yogyakarta



(Slamet Surinto)

HALAMAN PERSEMBAHAN

Karya ini kupersembahkan untuk Bapak dan Ibu, Mbak Ita, M shoffa, Mbak Lina, Mas Heru, Om Heic, Mbak Takpit, MY Lady serta semua Keponakanku Mbak awa, Coco, Chaca, Pia. Terima kasih atas semangat dan bimbingannya sehingga karya ini dapat terwujud

KATA PENGANTAR



Puji Syukur penulis panjatkan ke hadirat Allah SWT, Tuhan semesta alam, karena atas berkat rahmat-Nyalah penulis dapat dan mampu menyelesaikan skripsi ini yang merupakan tugas akhir pada Fakultas Teknik Jurusan Teknik Elektro Universitas Muhammadiyah Yogyakarta dengan judul :

“ IMPLEMENTASI SISTEM DETEKSI PENYUSUPAN PADA JARINGAN KOMPUTER ”.

Meskipun penulis telah berusaha sekuat tenaga dan mencurahkan segala pikiran yang ada untuk dapat menyajikan skripsi ini sebaik-baiknya, namun hasil yang penulis capai masih jauh dari sempurna.

Penulis mengucapkan terimakasih kepada semua pihak yang telah membantu dalam penulisan skripsi ini baik secara langsung maupun tidak langsung. Penulis juga tidak lupa mengucapkan terimakasih kepada :

1. Bapak Ir. Tony K Haryadi sebagai Dekan Fakultas Teknik
2. Bapak Ir. Slamet Suropto sebagai Kepala Jurusan Teknik Elektro
3. Bapak Ir. Dwijoko Purbohadi, MT, Dosen Pembimbing Utama.
4. Bapak Helmi Zain Nuri, ST, MT., Dosen Pembimbing Muda.
5. Keluarga penulis terutama Bapak dan Ibu yang telah memberikan dorongan moril yang tak ternilai harganya dalam menyelesaikan studi.
6. Mbak Ita, Mbak Lina, Mas Shoffa, Mas Heru, OM Heic, Mbak Ta'pit,

7. Tim Puma, Si Boy, Meican, Ling-ling, Krista, Menuk, Pohan dan Hawa
8. Teman-teman Inherent dan ITRG (Riri, Lilis, Ipulxd, Mas Mirwan, Bambang) terimakasih untuk kebersamaan dan pengalamannya selama ini
9. Keluarga besar BPSI UMY, Bapak Nafi, Bapak Wahyudi, Mas Andi, Mas Imenc, Mas Caka, Mas Yaom, Mas Caka, Mas Suwandi, Nugroho dan Hendri terimakasih buat pengalaman dan fasilitasnya.
10. Kru SAT.NET Yogyakarta Mas Anang, Mas Jajat, Pak Pras, Mas Santo, Mas Budi, Mas John, Rika, Arfa, Maskur maju terus pantang mundur.
11. Mylady terima kasih untuk motivasi dan semangatnya.
12. Semua pihak yang telah membantu penulis dalam menyelesaikan skripsi ini.

Penulis menyadari adanya kekurangan dalam penulisan skripsi ini, untuk itu dengan segala kerendahan hati penulis mengharapkan tegur sapa dan koreksi serta saran-saran dari para pembaca.

Akhir kata semoga segala maksud dan i'tikad baik senantiasa

... dengan Allah SWT Amin

Daftar Isi

KATA PENGANTAR	vii
Daftar Isi.....	ix
Daftar Gambar.....	xii
Daftar Tabel.....	xiii
BAB I PENDAHULUAN.....	1
A. Latar Belakang	1
B. Rumusan Masalah	3
C. Batasan Masalah.....	4
D. Tujuan	4
E. Kontribusi.....	4
BAB II LANDASAN TEORI.....	6
A. Sistem Deteksi Penyusupan	6
1. Pengertian Sistem Deteksi Penyusupan.....	6
2. Jenis-jenis <i>Intrusion Detection System</i>	6
B. Keamanan Jaringan Komputer	15
BAB III METODOLOGI.....	18
A. Prosedur Penelitian.....	18
B. Analisis Kebutuhan.....	19

C. Spesifikasi Sistem.....	19
D. Desain dan Implementasi.....	20
E. Validasi	24
BAB IV IMPLEMENTASI DAN PENGUJIAN	28
A. Pengujian Sistem Sebelum Dipasang di Jaringan Komputer.....	28
1. Pengujian Menggunakan NMAP	30
2. Pengujian Menggunakan Net Tools	32
B. Pengujian di Jaringan Komputer	34
1. Analisis Serangan menggunakan ACID.....	36
2. Performa Sistem	58
BAB V KESIMPULAN DAN SARAN.....	64
A. Kesimpulan	64
B. Saran	64
DAFTAR PUSTAKA	66
LAMPIRAN A INSTALASI DAN KONFIGURASI SISTEM PADA	
WINDOWS SERVER 2003.....	68
LAMPIRAN B PROSES INSTALASI DAN KONFIGURASI PADA	
SERVER CENTOS 4.3	116

Daftar Gambar

Gambar 2. 1 Arsitektur <i>Network Intrusion Detection System</i>	9
Gambar 2. 2 <i>Paket Sniffer</i>	10
Gambar 2. 3 Proses Pengkodean Paket.....	11
Gambar 2. 4 Cara kerja <i>detection engine</i>	11
Gambar 2. 5 Struktur <i>Rules</i>	12
Gambar 2. 6 Sistem IDS dengan menggunakan <i>web interface</i>	15
Gambar 3. 1 Diagram Prosedur Penelitian	19
Gambar 3. 2 Desain <i>Intrusion Detection System</i>	20
Gambar 3. 3 Pengujian Sistem Sebelum Ditempatkan di Dalam Jaringan Komputer	24
Gambar 3. 4 Nmap Melakukan Scanning Terhadap Suatu <i>Host</i>	25
Gambar 3. 5 Net Tools.....	25
Gambar 4. 1 Pengujian Sistem Sebelum Ditempatkan di Dalam Jaringan Komputer	29
Gambar 4. 2 Nmap Melakukan Scanning Pada Host Target	30
Gambar 4. 3 Log IDS Mendeteksi TCP <i>Port Scan</i> Yang Dilakukan NMAP	31
Gambar 4. 4 Penetrasi Menggunakan HTTP Subnet Scanner	32
Gambar 4. 5 Tampilan ACID Mendeteksi <i>Webserver Scanner</i> Yang Dilakukan Net Tools.....	33
Gambar 4. 6 Posisi Server <i>Intrusion Detection System</i> Pada Jaringan Komputer	35

Gambar 4. 8 Informasi mengenai <i>database</i> ACID.....	37
Gambar 4. 9 Menu ACID.....	38
Gambar 4. 10 Halaman Informasi mengenai sensor yang digunakan.	39
Gambar 4. 11 <i>Unique Alert</i>	40
Gambar 4. 12 Klasifikasi <i>alert</i> oleh ACID.....	41
Gambar 4. 13 Total <i>Alert</i> pada ACID.....	42
Gambar 4. 14 Alamat IP Sumber	43
Gambar 4. 15 Alamat IP Tujuan	44
Gambar 4. 16 <i>Unique</i> IP link.	45
Gambar 4. 17 ACID <i>Maintenance</i>	46
Gambar 4. 18 <i>Time Profile Of Alert</i>	48
Gambar 4. 19 <i>Alert Group</i>	49
Gambar 4. 20 Pencarian Frekuensi <i>Alert</i>	50
Gambar 4. 21 <i>Search</i> Parameter.....	51
Gambar 4. 22 <i>Search Signature NMAP</i>	51
Gambar 4. 23 Notifikasi melalui email.....	53
Gambar 4. 24 Perfoma Windows Server 2003.....	59
Gambar 4. 25 Perfoma CentOS 4.3	60

Daftar Tabel

Tabel 2. 1 Informasi <i>Rules</i> IDS	12
Tabel 4. 1 Setting IP Sebelum di Pasang di Jaringan Komputer.....	29
Tabel 4. 2 Setting IP <i>Address</i> Untuk Pengujian di Jaringan Komputer	34
Tabel 4. 3 <i>Alert</i> dan Klasifikasi Hasil Penelitian	54

vi