

**PERANCANGAN DAN REALISASI SISTEM KEAMANAN TERHADAP
PENYUSUPAN DAN SERANGAN PADA JARINGAN KOMPUTER
(STUDI KASUS NETWORK OPERATION CENTER UNIVERSITAS
KRISTEN MARANATHA BANDUNG)**

Disusun Oleh :

Nama : Gabriel Sebastian Wangsadipura

NRP : 0522084

Jurusan Teknik Elektro, Fakultas Teknik, Universitas Kristen Maranatha Bandung

Jln. Prof. Drg. Suria Sumantri, MPH no. 65, Bandung, Indonesia

Email : gabriel@gabrielsw.com

ABSTRAK

Berkembangnya teknologi informasi khususnya jaringan komputer dan layanan-layanannya di satu sisi mempermudah pekerjaan-pekerjaan manusia sehari-hari, akan tetapi di sisi lain timbul masalah yang sangat serius, yakni faktor keamanannya. Di satu sisi manusia sudah sangat tergantung dengan teknologi informasi, akan tetapi di sisi lain statistik kejahatan *cyber* meningkat tajam. Hal ini secara umum terjadi karena kepedulian terhadap keamanan sistem informasi masih sangat kurang. Network Operation Center Universitas Kristen Maranatha, sebagai suatu biro yang melakukan pemeliharaan terhadap jaringan komputer di Universitas Kristen Maranatha juga membutuhkan suatu sistem keamanan jaringan yang baik terhadap serangan dan penyusupan baik dari sisi *external* maupun *internal*.

Pada Tugas Akhir ini, sistem keamanan yang dibuat, dirancang untuk mengamankan suatu jaringan baik dari gangguan dari sisi internal maupun external. Sistem keamanan ini menggunakan IPS/IDS sebagai sistem pendeteksi dan pencegahan gangguan pada jaringan, WSUS untuk melakukan update pada operating system sehingga operating system tidak memiliki celah keamanan yang dapat disusupi oleh virus dan Symantec Endpoint Protection untuk mengamankan client dari virus atau Trojan.

Kata Kunci : Sistem Keamanan, Jaringan Komputer, IPS/IDS, Gangguan Pada Jaringan, Update Services, Virus.

**DESIGN AND REALIZATION OF SECURITY SYSTEM TOWARDS
INFILTRATION AND INCURSION IN COMPUTER NETWORK (CASE
STUDY AT NETWORK OPERATION CENTER MARANATHA
CHRISTIAN UNIVERSITY BANDUNG)**

Composed By :

Name : Gabriel Sebastian Wangsadipura

NRP : 0522084

Electrical Engineering Department, Maranatha Christian University Bandung

Jln. Prof. Drg. Suria Sumantri, MPH no. 65, Bandung, Indonesia

Email : gabriel@gabrielsw.com

ABSTRACT

Development in information technology especially computer networking and its service in one side make easier daily human job, but in another side appear serious problems, there is security factor. In one side, humans have been very dependent on information technology, but in other side, statistics of cyber crime increased sharply. This generally occurs because of concern for information security system is still very poor. Network Operation Center Maranatha Christian University, as a bureau which maintain computer networks in Maranatha Christian University needs a network security system which good against infiltration and attacks from both the external and internal side.

In this final project, security system which made, designed to secure a network from intrusion from either the internal or external side. This security system uses IPS / IDS system as detector and prevention intrusion on the network, WSUS to update the operating system so that the operating system does not have a security hole that can be infiltrated by the virus and Symantec Endpoint Protection to secure the client's from both of virus and Trojan.

Kata Kunci : Security System, Computer Networking, IPS/IDS, Intrusion At Network, Update Services, Virus.

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yesus Kristus karena atas berkat rahmat-Nya dan kasih karunia-Nya penulis dapat menyelesaikan laporan tugas akhir ini.

Laporan Tugas Akhir ini berjudul “ Perancangan Dan Realisasi Sistem Keamanan Terhadap Penyusupan Dan Serangan Pada Jaringan Komputer (Studi Kasus Network Operation Center Universitas Kristen Maranatha Bandung)” diajukan untuk memenuhi persyaratan dalam menempuh program pendidikan sarjana Stata 1 (S-1) pada Fakultas Teknik Jurusan Teknik Elektro, Universitas Kristen Maranatha.

Tugas Akhir ini diselesaikan dalam waktu yang cukup. Tanpa hikmat dan anugerah Tuhan, serta bantuan dari berbagai pihak, tidak mungkin tugas akhir ini dapat diselesaikan dengan baik. Oleh karena itu penulis mengucapkan terima kasih kepada pihak-pihak yang telah membantu dalam pengerjaan tugas akhir ini :

1. Bapak Heri Andrianto, S.T, M.T., selaku pembimbing utama yang telah bersedia meluangkan waktu untuk memberikan bimbingan serta pengarahannya.
2. Bapak Teja Andy Suardi, S.T., selaku pembimbing kedua dan Kepala Network Operation Center Universitas Kristen Maranatha Bandung, untuk kesempatan mengerjakan Tugas Akhir di Network Operation Center, untuk bimbingan, pembekalan ilmu mengenai jaringan komputer, sehingga tugas akhir ini dapat terselesaikan.
3. Bapak Ir. Aan Darmawan, M.T., Bapak Agus Prijono, S.T.,M.T. dan Bapak Dr. Ir. Daniel Setadikarunia, M.T. selaku penguji tugas akhir yang telah memberikan saran, ide dan kritik pada saat seminar dan sidang tugas akhir.
4. Bapak Dr. Ir. Daniel Setiadikarunia, M.T., selaku Ketua Jurusan Teknik Elektro Universitas Kristen Maranatha.

5. Ibu Ir. Anita Soepariono, M.Sc., selaku Koordinator Tugas Akhir Jurusan Teknik Elektro Universitas Kristen Maranatha atas bantuan serta bimbingannya dalam menyusun dan mengajukan proposal.
6. Seluruh staff jurusan Teknik Elektro Universitas Kristen Maranatha Bandung, yang telah membatu penulis dalam pengurusan administrasi tugas akhir.
7. Keluarga besar penulis khususnya kepada Papah, Mamah dan Randhy yang telah memberikan dukungan baik moral, materil serta doa sehingga tugas akhir ini dapat diselesaikan dengan baik.
8. Rekan kerja di Network Operation Center Universitas Kristen Maranatha, Irsan, S.Kom, Hendrik, S.Kom, Ansen, Dewi, S.T., Erika, S.T., Nola, Nico, Morris, Enrico A, S.Kom., Charles, Hendry K, Ferry, Chris yang mendukung penulis untuk menyelesaikan tugas akhir ini dan dukungan resource baik software maupun hardware yang tersedia, sehingga penulis dapat menyelesaikan tugas akhir ini.
9. Kepada teman – teman dekat Edsel, Irene, Irwin, Johanes, Lusi, Maya, Melly, Michael, Niko, Pamella, Rhendy, Stevanus atas dorongan semangat dan doanya.
10. Linda Agustina Surono, you're the inspiration that made my fingers type and my brain think.

Penulis menyadari bahwa laporan tugas akhir ini jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang bersifat membangun untuk kemajuan dan kesempurnaan di masa yang akan datang .

Akhir kata, semoga laporan tugas akhir ini dapat bermanfaat dan berguna bagi kemajuan almamater dan menjadi sumbangan pikiran bagi semua pihak.

Bandung, Agustus 2009

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR GAMBAR.....	viii
DAFTAR TABEL	xii
BAB I PENDAHULUAN	
I.1 Latar Belakang.....	1
I.2 Identifikasi Masalah.....	2
I.3 Perumusan Masalah.....	2
I.4 Tujuan	3
I.5 Pembatasan Masalah.....	3
I.6 Spesifikasi Sistem.....	3
I.7 Sistematika Penulisan	4
BAB II LANDASAN TEORI	
II.1 Model OSI	5
II.1.1 Pengorganisasian Lapisan	6
II.1.2 Lapisan OSI.....	7
II.1.3 Interaksi Antar Layer Pada OSI	9
II.2 Jaringan Komputer.....	10
II.2.1. Jenis Jaringan	11
II.2.2. Mode Operasi Jaringan.....	12
II.2.3 IP Address	13

II.3	Protokol TCP/IP.....	15
II.4	Firewall	17
II.4.1	Karakteristik Firewall.....	18
II.5	Sistem Pencegahan Penyusupan (IPS).....	19
II.6	SNORT IDS.....	21
BAB III PERANCANGAN DAN REALISASI		
III.1	Cara Kerja Sistem.....	24
III.2	Perancangan Sistem Keamanan.....	25
III.3	Instalasi Dan Konfigurasi IPS/IDS.....	26
III.4	Instalasi Dan Konfigurasi Symantec Endpoint Protection Server.....	35
III.5	Instalasi Dan Konfigurasi Windows Server Update Services	44
BAB IV ANALISA DAN DATA PENGAMATAN		
IV.1	Pengujian IPS/IDS	55
IV.1.1	Pengujian Dengan Scanning Port Melalui Jaringan Internal	55
IV.1.2	Pengujian Dengan Scanning Port Melalui Jaringan External	58
IV.2	Pengujian Symantec Endpoint Protection	61
IV.2.1	Pengujian Installasi Symantec Endpoint Protection Menggunakan Silent Mode.....	61
IV.2.2	Pengujian Installasi Symantec Endpoint Protection Menggunakan File Setup Per Domain.....	65
IV.3	Pengujian Windows Server Update Services	68
BAB V KESIMPULAN DAN SARAN		
V.1	Kesimpulan.....	71
V.2	Saran	72
DAFTAR PUSTAKA		73

LAMPIRAN A SOURCE CODE REGISTRY WSUS

LAMPIRAN B SNORT RULES

DAFTAR GAMBAR

Gambar 2.1 Model OSI Layer	5
Gambar 2.2 Lapisan - Lapisan Pada OSI Layer	6
Gambar 2.3 Ilustrasi Routing	7
Gambar 2.4 Proses Komunikasi OSI Layer	9
Gambar 2.5 Susunan Protokol TCP/IP	16
Gambar 2.6 Ilustrasi Firewall	18
Gambar 2.7 Hubungan Komponen – Komponen SNORT IDS	23
Gambar 3.1 Jaringan Universitas Kristen Maranatha.....	24
Gambar 3.2 Skema Jaringan Universitas Kristen Maranatha Dengan Sistem Kemanan Tambahan	26
Gambar 3.3 Pemasangan Snort 1	27
Gambar 3.4 Pemasangan Snort 2	27
Gambar 3.5 Pemasangan Snort 3	27
Gambar 3.6 Pemasangan Snort 4	28
Gambar 3.7 Pemasangan Snort 5	28
Gambar 3.8 Pemasangan BASE 1	28
Gambar 3.9 Pemasangan BASE 2	29
Gambar 3.10 Pemasangan BASE 3	29
Gambar 3.11 Pemasangan BASE 4	30
Gambar 3.12 Pemasangan BASE 5	30
Gambar 3.13 Pemasangan BASE 6	31
Gambar 3.14 Proses Pengaktifan Snort	31
Gambar 3.15 Tampilan BASE Ketika Snort Telah Aktif.....	32

Gambar 3.16 Proses Pemasangan BlockIt 1	33
Gambar 3.17 Proses Pemasangan BlockIt 2.....	33
Gambar 3.18 Proses Pemasangan BlockIt 3.....	34
Gambar 3.19 Proses Pemasangan BlockIt 4.....	34
Gambar 3.20 Proses Pemasangan BlockIt 6.....	35
Gambar 3.21 Proses Pemasangan Symantec Endpoint Protection Server 1	36
Gambar 3.22 Proses Pemasangan Symantec Endpoint Protection Server 2	36
Gambar 3.23 Proses Pemasangan Symantec Endpoint Protection Server 3	37
Gambar 3.24 Proses Pemasangan Symantec Endpoint Protection Server 4	37
Gambar 3.25 Proses Pemasangan Symantec Endpoint Protection Server 5	38
Gambar 3.26 Proses Pemasangan Symantec Endpoint Protection Server 6	38
Gambar 3.27 Proses Pemasangan Symantec Endpoint Protection Server 7	39
Gambar 3.28 Proses Pemasangan Symantec Endpoint Protection Server 8	39
Gambar 3.29 Proses Pemasangan Symantec Endpoint Protection Server 9	40
Gambar 3.30 Proses Pemasangan Symantec Endpoint Protection Server 10	40
Gambar 3.31 Proses Pemasangan Symantec Endpoint Protection Server 11	41
Gambar 3.32 Proses Pemasangan Symantec Endpoint Protection Server 12	41
Gambar 3.33 Proses Pemasangan Symantec Endpoint Protection Server 13	42
Gambar 3.34 Proses Pemasangan Symantec Endpoint Protection Server 14	42
Gambar 3.35 Pengaturan Pada Symantec Endpoint Protection Manager 1	43
Gambar 3.36 Pengaturan Pada Symantec Endpoint Protection Manager 2	43
Gambar 3.37 Pengaturan Pada Symantec Endpoint Protection Manager 3	44
Gambar 3.38 Pemasangan Windows Server Update Services 1	45
Gambar 3.39 Pemasangan Windows Server Update Services 2	45
Gambar 3.40 Pemasangan Windows Server Update Services 3	46

Gambar 3.41 Pemasangan Windows Server Update Services 4	46
Gambar 3.42 Pemasangan Windows Server Update Services 5	47
Gambar 3.43 Pemasangan Windows Server Update Services 6	47
Gambar 3.44 Pemasangan Windows Server Update Services 7	48
Gambar 3.45 Pemasangan Windows Server Update Services 8	48
Gambar 3.46 Pemasangan Windows Server Update Services 9	49
Gambar 3.47 Pemasangan Windows Server Update Services 10	49
Gambar 3.48 Pemasangan Windows Server Update Services 11	50
Gambar 3.49 Pemasangan Windows Server Update Services 12	50
Gambar 3.50 Pemasangan Windows Server Update Services 13	51
Gambar 3.51 Pemasangan Windows Server Update Services 14	51
Gambar 3.52 Pemasangan Windows Server Update Services 15	52
Gambar 3.53 Pemasangan Windows Server Update Services 16	52
Gambar 3.54 Pemasangan Windows Server Update Services 17	53
Gambar 3.55 Pemasangan Windows Server Update Services 18	53
Gambar 3.56 Pemasangan Windows Server Update Services 19	54
Gambar 4.1 Tampilan Pada IpTables Sebelum Dilakukan Port Scanning	56
Gambar 4.2 Tampilan Pada Saat Proses Port Scanning	57
Gambar 4.3 Tampilan Pada IpTables Setelah Proses Port Scanning	57
Gambar 4.4 Tampilan Pada IPTables Sebelum Dilakukan Scanning Port	59
Gambar 4.5 Proses Scanning Port Menggunakan SuperScan	59
Gambar 4.6 Pada IPTables Setelah Scanning Port Dilakukan	60
Gambar 4.7 Tampilan Symantec Endpoint Manager Console	62
Gambar 4.8 Window Untuk Memasukkan Password Dan Username.....	62
Gambar 4.9 Status Installasi Pada Client Telah Selesai	63

Gambar 4.10 Tampilan Pada PC Clie setelah Symantec Endpoint Protection Berhasil Terinstall	63
Gambar 4.11 Tampilan Menu Pembuatan Setup Package	65
Gambar 4.12 Window Untuk Membuat Setup Package.....	65
Gambar 4.13 Proses Pembuatan Setup Package.....	66
Gambar 4.14 Setup Package Yang Telah Dibuat Untuk Tiap Domain.....	66
Gambar 4.15 Tampilan Pada Client Yang Telah Terinstall Symantec Endpoint Protection.....	66
Gambar 4.16 Proses Update Untuk Client Yang Tergabung Dalam Domain	69
Gambar 4.17 Proses Pengupdaten Secara Manual Pada Client Yang Tidak Tergabung Dalam Domain	69

DAFTAR TABEL

Tabel 4.1 Proses Pengujian Serangan Terhadap IPS/IDS Dengan Melakukan Port Scanning Menggunakan Tools Super Scan Melalui Jaringan Internal.....	58
Tabel 4.2 Proses Pengujian Serangan Terhadap IPS/IDS Dengan Melakukan Port Scanning Menggunakan Tools Super Scan Melalui Jaringan External.....	60
Tabel 4.3 Tabel Pengujian Pemasangan Symantec Endpoint Protection Pada Client Dengan Menggunakan Symantec Endpoint Protection Manager.....	64
Tabel 4.4 Tabel Pengujian Pemasangan Symantec Endpoint Protection Pada Client Dengan Menggunakan Setup Package.....	67
Tabel 4.5 Tabel Pengujian Pengaturan Windows Update Pada Client Yang Terhubung Dalam Domain Untuk Terhubung Pada WSUS.....	70
Tabel 4.6 Tabel Pengujian Pengaturan Windows Update Pada Client Yang Tidak Terhubung Dalam Domain Untuk Terhubung Pada WSUS.....	70