

KATA PENGANTAR

Alhamdulillah, segala puji dan syukur penulis panjatkan kepada Allah Subhanahu wa Ta'ala atas segala rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul “Sistem Pencegahan Flooding Data dan Blocking IP secara Otomatis pada Jaringan Komputer” dengan baik. Skripsi ini disusun untuk memenuhi sebagian persyaratan memperoleh gelar Sarjana Teknik di Jurusan Teknik Elektro Program Studi Teknik Informatika dan Komputer Fakultas Teknik Universitas Brawijaya. Penulis ingin mengucapkan terima kasih kepada beberapa pihak yang telah membantu dan mendukung dalam penyelesaian skripsi ini, yaitu:

1. Ayahanda Drs. Heru Harsono MSc, dan Ibunda Tercinta Dra. Zahratul Jannah AR MSc, atas segala doa, dukungan, dan kasih sayang yang tiada henti yang diberikan pada ananda hingga saat ini. Maafkan Ananda belum mampu membalas semuanya. Semoga Allah Yang Maha Agung memberikan ruang surga untuk kedua orang tua tercinta.
2. Kakak Diaz Zulmy Hariza dan adik tercinta Diandra Alifatus Shafira, untuk seluruh dukungan yang berarti.
3. Sahabat terbaik Illosa dan Illona, terima kasih untuk semuanya dukungannya di masa-masa sulit. Tidak ada yang bisa membalas semua kebaikan kalian selain Tuhan di Atas. *Best friends forever yah!*
4. Bapak Ir. Heru Nurwarsito, M.Kom selaku Ketua Jurusan Teknik Elektro dan Bapak Rudy Yuwono, ST., M.Sc. selaku Sekretaris Jurusan Teknik Elektro, atas semua kemudahan yang telah diberikan.
5. Bapak Arief Andy Soebroto, ST., M.Kom selaku KKDK Teknik Informatika dan Komputer.
6. Bapak Raden Arief Setyawan ST., MT. dan Bapak Himawat Aryadita ST., MT., MSc selaku dosen pembimbing yang telah banyak memberikan bimbingan dan arahan terhadap penyusunan skripsi ini.
7. Staf Pengajar, Administrasi, dan Perpustakaan Jurusan Teknik Elektro Fakultas Teknik Universitas Brawijaya, terutama Mas Aris, Mbak Frida, dan Mbak Heni,

Pak Heru, terima kasih sebesar-besarnya telah bersedia bersusah payah membantu segala urusan administrasi kami.

8. Teman-teman angkatan 2002, atas dukungan dan motivasinya.
9. Semua pihak yang tidak dapat disebutkan satu persatu di sini, yang telah membantu penyelesaian skripsi ini.

Semoga Allah SWT memberikan karunia dan hidayah serta balasan kebahagiaan dan kesuksesan atas segala budi baik pihak-pihak yang telah mendukung penulis selama ini.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan dan masih jauh dari sempurna, untuk itu saran dan kritik yang membangun sangat penulis harapkan. Semoga skripsi ini membawa manfaat bagi penulis maupun pihak lain yang menggunakannya.



Malang, Juli 2009

Penulis

DAFTAR ISI

PENGANTAR	i
DAFTAR ISI	iii
DAFTAR GAMBAR	ix
DAFTAR TABEL	xi
ABSTRAK	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Ruang Lingkup Pembahasan	3
1.4 Tujuan Penulisan	3
1.5 Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA	5
2.1 Jaringan Komputer	5
2.1.1 Sejarah Jaringan Komputer	7
2.1.2 Tipe Jaringan Komputer	8
2.1.2.1 Tipe Jaringan Komputer Menurut Fungsinya	8
2.1.2.1.1 Jaringan Peer to Peer	8
2.1.2.1.2 Jaringan Client-Server	9
2.1.2.2 Tipe Jaringan Komputer Menurut Cakupan Geografis	9
2.1.2.2.1 LAN (Local Area Network)	10
2.1.2.2.2 MAN (Metropolitan Area Network)	10
2.1.2.2.3 WAN (Wide Area Network)	11
2.1.2.2.4 GAN (Global Area Network)	11

2.1.3	Topologi Jaringan Komputer	13
2.1.3.1	Topologi Bus	13
2.1.3.2	Topologi Ring	14
2.1.3.3	Topologi Star	14
2.2	OSI (Open System Interconnection)	15
2.2.1	Model Referensi OSI	15
2.2.2	Karakteristik Lapisan OSI	18
2.2.3	Protocol	19
2.2.4	Lapisan-lapisan Model OSI	20
2.2.4.1	Physical Layer	20
2.2.4.2	Data Link Layer	20
2.2.4.3	Network Layer	21
2.2.4.4	Transport Layer	22
2.2.4.5	Session Layer	24
2.2.4.6	Presentation Layer	24
2.2.4.7	Application Layer	25
2.2.5	Transmisi Data Pada Model OSI	26
2.3	Internet Protocol (IP)	27
2.3.1	Format Alamat IP	28
2.3.2	Macam-macam Protocol IP	28
2.3.2.1	Internet Control Message Protocol (ICMP)	28
2.3.2.1.1	Format Header ICMP	29
2.3.2.2	User Datagram Protocol (UDP)	31
2.3.2.2.1	Format Header UDP	32



2.3.2.3	Transmission Control Protocol (TCP)	33
2.3.2.3.1	Format Header TCP	34
2.4	TCP/IP	37
2.4.1	Layanan TCP/IP	39
2.4.1.1	Pengiriman File (Transfer File)	39
2.4.1.2	Remote Login	39
2.4.1.3	Computer Mail	39
2.4.1.4	Network File System (NFS)	39
2.4.1.5	Remote Execution	39
2.4.1.6	Name Server	40
2.4.2	Arsitektur TCP/IP	40
2.4.2.1	Network Access Layer	40
2.4.2.2	Internet Layer	41
2.4.2.3	Transport Layer	41
2.4.2.4	Application Layer	42
2.5	Keamanan Jaringan Komputer	43
2.5.1	Flood Data	43
2.6	Intrusion Detection System (IDS)	45
2.6.1	Host Intrusion Detection System (HIDS)	45
2.6.2	Network Intrusion Detection System(NIDS)	46
2.6.3	Knowledge Based IDS	47
2.6.4	Behaviour Based IDS	48
2.7	Snort	48
2.8	Metode Pengambilan Data	50

2.9	Metode Pemblokiran IP	53
BAB III METODE PENELITIAN		55
3.1	Studi Literatur	55
3.2	Perancangan dan Implementasi Sistem	56
3.3	Pengujian dan Analisis Sistem	56
3.4	Pengambilan Kesimpulan dan Saran	56
BAB IV ANALISIS DAN PERANCANGAN		57
4.1	Analisis Sistem	58
4.1.1	Analisis Kebutuhan	58
4.1.1.1	Definisi Konseptual	59
4.1.1.2	Penentuan Kebutuhan Fungsional	59
4.1.2	Spesifikasi Kebutuhan	60
4.1.3	Analisis Context Diagram dan Data Flow Diagram (DFD)	61
4.1.3.1	DFD Level 0 Client ke Router	62
4.1.3.2	DFD Level 1 Client ke server	63
4.2	Perancangan Sistem	66
4.2.1	Spesifikasi Sistem	66
4.2.2	Perancangan Diagram Sistem	67
4.2.2.1	Desain Sistem Secara Umum	67
4.2.3	Perancangan Diagram Jaringan	68
4.2.4	Desain Pemblokiran IP	69
4.2.5	Perancangan Rules Snort	70
4.2.6	Perancangan Firewall	71
4.2.6.1	BlockIt	71

4.2.6.2 Iptables	71
BAB V IMPLEMENTASI	72
5.1 Implementasi Jaringan Komputer	73
5.1.1 Perangkat Keras Jaringan Komputer	73
5.1.2 Perangkat Lunak Jaringan Komputer	74
5.1.2.1 Konfigurasi Komputer Router	74
5.1.2.2 Konfigurasi TCP/IP pada Komputer Client	77
5.1.2.3 Konfigurasi TCP/IP pada Komputer Penyerang	78
5.2 Implementasi Perangkat Lunak	79
5.2.1 Instalasi Snort	79
5.2.1.1 Patching	80
5.2.1.2 Konfigurasi Snort	80
5.2.1.3 Rules Snort	80
5.2.2 Instalasi Paket Library	82
5.2.3 Instalasi Firewall	85
5.2.3.1 Instalasi BlockIt	85
5.2.3.2 konfigurasi BlockIt	85
5.2.4 Konfigurasi NAT	87
BAB VI PENGUJIAN	88
6.1 Spesifikasi Komputer Pengujian	88
6.2 Pengujian DoS (Denial of Service)	89
6.2.1 Pengujian Ping Flood dari network internal	90
BAB VII KESIMPULAN DAN SARAN	97
7.1 Kesimpulan	97



7.2 Saran98

DAFTAR PUSTAKA99



DAFTAR GAMBAR

Gambar 2.1	Jaringan <i>peer to peer</i>	8
Gambar 2.2	Jaringan <i>Client – Server</i>	9
Gambar 2.3	Jaringan MAN	10
Gambar 2.4	Jaringan WAN	11
Gambar 2.5	Jaringan GAN	12
Gambar 2.6	interaksi antara LAN, MAN, WAN, GAN	12
Gambar 2.7	jaringan dengan topologi bus	13
Gambar 2.8	jaringan dengan topologi ring	14
Gambar 2.9	jaringan dengan topologi star	15
Gambar 2.10	Contoh tentang bagaimana model OSI digunakan	27
Gambar 2.11	Format Header ICMP	29
Gambar 2.12	Format Header UDP	32
Gambar 2.13	Pseudoheader UDP	33
Gambar 2.14	Format Header TCP	34
Gambar 2.15	Pseudoheader TCP	36
Gambar 2.16	Arsitektur TCP/IP	40
Gambar 2.17	Proses data TCP	44
Gambar 2.18	Host Based IDS	46
Gambar 2.19	Network Based IDS	47
Gambar 2.20	Jaringan pada Hub	51
Gambar 2.21	Jaringan pada Switch	52

Gambar 2.22	IPSECPOL pada tampilan windows	54
Gambar 4.1	Diagram Pohon Perancangan	57
Gambar 4.2	DFD Level 0	62
Gambar 4.3	DFD level 1 Client ke Server	64
Gambar 4.3	Urutan Paket IP	66
Gambar 4.4	Desain umum program blokir otomatis pada flood	67
Gambar 4.5	Desain perancangan jaringan sistem	68
Gambar 4.6	Desain blokir IP	69
Gambar 4.7	Rules Snort	70
Gambar 5.1	Implementasi Sistem Pencegahan Flooding Data	72
Gambar 5.2	Konfigurasi IP Address pada Client	78
Gambar 5.3	Konfigurasi IP Address pada Komputer Penyerang	79
Gambar 6.1	Ping Flood dari komputer penyerang network internal saat Snort tidak aktif	91
Gambar 6.2	Iptables meloloskan alamat IP komputer penyerang (network internal) Saat melakukan ping flood	92
Gambar 6.3	Flood dari komputer penyerang network internal saat Snort aktif	93
Gambar 6.4	Snort mendeteksi ping flood dari komputer penyerang network internal	94
Gambar 6.5	Blockit mencatat IP komputer penyerang network internal yang melakukan ping Flood	95
Gambar 6.6	Iptables memblok alamat IP komputer penyerang network internal yang melakukan ping flood	96

DAFTAR TABEL

Tabel 2.1	Model OSI	16
Tabel 2.2	Lapisan TCP/IP	17
Tabel 2.3	Pemisahan Lapisan Atas dan Lapisan Bawah pada Model OSI	19



ABSTRAK

DEVY RIZKA, 2009 : Sistem Pencegahan Flooding Data dan Blocking IP secara Otomatis pada Jaringan Komputer. Skripsi Jurusan Teknik Elektro , Fakultas Teknik, Universitas Brawijaya. Dosen Pembimbing : R. Arief Setyawan ST., MT dan Himawat Aryadita ST., MT., MSc

Seiring dengan perkembangan teknologi pada dunia internet, fungsi dari internet pun berkembang dimana internet menyediakan akses untuk layanan telekomunikasi dan sumber daya informasi untuk jutaan pemakainya yang tersebar di seluruh dunia. Akan tetapi tak hanya keuntungan yang didapat dari berkembangnya penggunaan internet, tapi juga ada beberapa kelemahan, khususnya dalam faktor keamanan. Salah satu yang mengancam faktor keamanan tersebut adalah flooding data pada jaringan.

Dalam hal itu, maka diperlukan berbagai macam teknik-teknik pencegahan serangan pada jaringan, dalam kaitannya dengan faktor keamanan jaringan. Salah satunya adalah dengan sistem pencegahan flooding data, dengan menggunakan software Snort yang berbasis Host-based IDS, dan sistem blocking IP secara otomatis, dengan firewall IPTables. Sistem bekerja dengan membangun sebuah engine yang membaca parameter penyerangan dengan flooding dari IP penyerang, kemudian sistem memberikan alert yang kemudian akan memerintahkan IPTables firewall untuk melakukan blocking akses pada IP penyerang tersebut.

Pengujian terhadap perancangan dan implementasi sistem pencegahan flooding data ini dilakukan sampai pada titik dimana sistem aman terhadap ancaman adanya flooding data yang dapat menyebabkan sistem hang. Pengujian yang dilakukan adalah pengujian dengan metode ping flood. Pengujian ini memperlihatkan hasil status time out pada komputer penyerang. Hal ini menunjukkan sistem pencegahan flooding data pada jaringan telah dapat menghentikan serangan dan melakukan blocking IP secara otomatis terhadap computer penyerang.

Kata Kunci : Flooding Data, Sistem Pencegahan Flooding Data, Snort, Host-based IDS, IPTables, Firewall, Ping Flood