

KATA PENGANTAR



Puji dan syukur alhmandulillah pantas diucapkan kepada ALLAH SWT, yang telah memberikan petunjuk dalam menyelesaikan proyek akhir ini dengan judul “Implementasi Pencegahan Serangan *Interruption* Jenis *Flooding* terhadap Keamanan Layanan *Video Streaming* dan *Transfer File*”. Shalawat beriring salam diberikan kepada nabi besar Nabi Muhammad SAW.

Pembuatan proyek akhir ini telah mendapatkan banyak dukungan dari beberapa pihak sehingga proses pengerjaan proyek akhir ini dapat selesai. Atas dukungan yang telah diberikan, penulis ingin mengucapkan terimakasih kepada:

1. Ibu, Heni Kustianingsih dan Ayah, Harunsyah, yang telah memberikan pengorbanan besar sehingga penulis dapat menyelesaikan pendidikan akhir.
2. Bapak S.N.M.P Simamora selaku pembimbing I yang telah berkontribusi memberikan saran dan solusi atas masalah yang dihadapi penulis.
3. Bapak Anang Sularso selaku pembimbing II yang telah memberikan pengarahan dalam pengerjaan proyek akhir ini.
4. Teman – teman yang memberikan doa dan dukungan yang besar sehingga penulis mendapatkan semangat untuk mengerjakan proyek akhir ini.

Penulis menyadari bahwa buku atau implementasi proyek akhir ini belum mencapai kesempurnaan. Kritik dan saran yang membangun akan diterima oleh penulis untuk memperbaiki kesalahan yang sama. Semoga laporan proyek akhir ini dapat memberikan manfaat bagi pembaca.

Bandung, 4 Agustus 2011

Laila Nuzha Lubis

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
LEMBAR PERNYATAAN	iii
KATA PENGANTAR	iv
DAFTAR ISI	v
DAFTAR GAMBAR	vii
DAFTAR TABEL.....	ix
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	2
1.3 Tujuan.....	2
1.4 Batasan Masalah.....	3
BAB II.....	4
LANDASAN TEORI.....	4
2.1 <i>Client/server</i>	4
2.2 Kapasitas Kanal.....	5
2.3 Konsep <i>Streaming</i>	6
2.3.1 Cara Kerja <i>Video Streaming</i>	6
2.4 Keamanan Jaringan	7
2.5.1 Aspek-aspek Keamanan Komputer	7
2.5.2 Aspek-aspek Ancaman Keamanan	8
2.6 MRTG (<i>Multi Router Traffic Graph</i>)	8
2.7 <i>Denial of Service</i> (DOS).....	9
2.7.1 Metode Serangan <i>DoS Flooding</i>	10
BAB III.....	11
ANALISIS KEBUTUHAN DAN PERANCANGAN	11

3.1 Alur Kerja	11
3.2 Arsitektur Sistem.....	12
3.3 Deskripsi Sistem.....	12
3.3.1 Deskripsi Sistem Aplikasi <i>Video Streaming</i>	12
3.3.2 Deskripsi Sistem Keamanan Jaringan.....	13
3.4 Spesifikasi Sistem.....	15
3.4.1 Spesifikasi Perangkat Keras <i>Server</i>	15
3.4.2 Spesifikasi Perangkat Keras <i>Client</i>	15
3.4.3 Spesifikasi Perangkat Lunak	16
BAB IV	18
IMPLEMENTASI DAN PENGUJIAN.....	18
4.1 Implementasi.....	18
4.1.1 Implementasi <i>Web Server</i>	18
4.1.2 Implementasi <i>DNS Server</i>	19
4.1.3 Implementasi <i>FTP Server</i>	19
4.1.4 Implementasi <i>Hacker</i> (Penyerang)	20
4.2 Pengujian dan Analisis	20
4.2.1 Pengujian dan Analisis Fitur Pendukung Jaringan	20
4.2.2 Pengujian dan Analisis Sistem Penyerangan dan Pencegahan Serangan <i>Flooding</i>	28
4.2.3 Hasil Pengujian dan Analisis.....	35
BAB V.....	44
PENUTUP.....	44
5.1 Kesimpulan	44
5.2 Saran.....	44
DAFTAR PUSTAKA	
LAMPIRAN	

DAFTAR GAMBAR

Gambar 3.1 Alur Kerja Sistem	11
Gambar 3.2 Arsitektur Sistem	12
Gambar 3.3 Tahap-Tahap Keamanan Jaringan	13
Gambar 4.1 <i>Flowchart</i> implementasi <i>web server</i>	18
Gambar 4.2 Struktur <i>domainserver</i>	19
Gambar 4.3 Skenario pengujian DHCP <i>server</i>	20
Gambar 4.4 <i>Detail network address</i>	21
Gambar 4.5 Skenario pengujian DNS <i>Server</i>	22
Gambar 4.6 Tes DNS	23
Gambar 4.7 Skenario pengujian FTP <i>server</i>	24
Gambar 4.8 FTP <i>server</i>	24
Gambar 4.9 Skenario pengujian layanan <i>web server</i>	25
Gambar 4.10 IP <i>web server</i>	25
Gambar 4.11 <i>Interface website library</i>	26
Gambar 4.12 <i>Website video streaming</i>	27
Gambar 4.13 MRTG	27
Gambar 4.14 Tribe Flood Network	29
Gambar 4.15 Low Orbit Ion Cannon.....	29
Gambar 4.16 <i>Capture</i> tshark Ethernet1 sebelum <i>flooding</i>	31
Gambar 4.17 <i>Capture</i> wireshark Ethernet1 sebelum <i>flooding</i>	32
Gambar 4.18 <i>Capture</i> tshark Ethernet1 ketika <i>flooding</i>	32
Gambar 4.19 <i>Capture</i> wireshark Ethernet1 ketika <i>flooding</i>	34

Gambar 4.20 Skenario saat serangan <i>flooding</i> terjadi.....	35
Gambar 4.21 <i>Buffer video</i> saat <i>streaming</i>	37
Gambar 4.22 Proses <i>downloading file</i> dengan <i>bandwidth limited</i>	37
Gambar 4.23 Proses <i>downloading file</i> ketika <i>flooding</i>	38
Gambar 4.24 Skenario pertahanan <i>web server</i>	40
Gambar 4.25 <i>Forbidden access</i>	41
Gambar 4.26 <i>Webpage</i> tidak ditemukan	41

DAFTAR TABEL

Tabel 3.1 Spesifikasi perangkat keras <i>server</i>	15
Tabel 3.2 Spesifikasi perangkat keras <i>client</i>	15
Tabel 3.3 Spesifikasi perangkat keras <i>hacker</i>	16
Tabel 3.4 Spesifikasi perangkat lunak <i>web server</i>	16
Tabel 3.5 Spesifikasi perangkat lunak FTP <i>server</i>	16
Tabel 3.6 Spesifikasi perangkat lunak DNS <i>server</i>	16
Tabel 3.7 Spesifikasi perangkat lunak penyerang	17
Tabel 3.8 Spesifikasi perangkat lunak <i>client</i>	17
Tabel 3.9 Nilai <i>transfer-rate</i> saat kondisi normal	37
Tabel 4.0 Nilai <i>transfer-rate</i> saat <i>flooding</i> terjadi	38