

DAFTAR ISI

LEMBAR PENGESAHAN.....	i
ABSTRAK	ii
<i>ABSTRACT</i>	iii
LEMBAR PERNYATAAN ORISINALITAS	iv
KATA PENGANTAR.....	iii
LEMBAR PERSEMBAHAN	iv
DAFTAR ISI.....	v
DAFTAR GAMBAR.....	x
DAFTAR TABEL.....	xv
DAFTAR LAMPIRAN	xvii
DAFTAR ISTILAH.....	xviii
DAFTAR SINGKATAN.....	xv
BAB I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah.....	2
I.3 Tujuan Penelitian.....	2
I.4 Batasan Penelitian	3
I.5 Manfaat Penelitian.....	3
I.6 Sistematika Penulisan.....	3
BAB II TINJAUAN PUSTAKA.....	5
II.1 Keamanan Informasi.....	5
II.2 <i>Firewall</i>	5
II.3 Virtualisasi Fortigate.....	5
II.5 <i>Distributed Denial of service Attack (DDoS)</i>	7
II.5.1 <i>SYN flood</i>	7
II.5.2 Hping3.....	8
II.6 <i>Platform</i> Eksperimen	8
II.6.1 <i>Attacker Operating System Software</i>	8
II.6.2 Router.....	8

II.6.3 <i>Web Server</i>	9
II.7 <i>Flowchart</i>	9
II.8 <i>Load Testing</i>	9
II.9 Sumber Daya Komputasi	9
II.10 TCP <i>Three-Way Handshake</i>	9
II.11 <i>Profiling System</i>	10
II.12 Penelitian Terakhir	10
II.13 Penelitian Saat Ini	10
BAB III METODOLOGI PENELITIAN	12
III.1 Model Konseptual	12
III.2 Sistematika Penyelesaian Masalah	13
III.2.1 Tahap Perumusan Masalah	15
III.2.2 Tahap Hipotesis	15
III.2.3 Tahap Perancangan Pengujian	15
III.2.4 Tahap Pengujian	15
III.2.5 Tahap Analisis	16
III.2.6 Tahap Akhir	16
III.2 Pengumpulan Data	17
III.4 Pengolahan Data	17
III.5 Metode Evaluasi	17
BAB IV PERANCANGAN DAN SKENARIO PENGUJIAN	18
IV.1 Rancangan Sistem	18
IV.1.1 Spesifikasi <i>Hardware</i>	18
IV.1.2 Spesifikasi <i>Software</i>	19
IV.1.3 Topologi Eksperimen	20
IV.1.4 Daftar IP Address	21
IV.2 Skenario Pengujian	21
IV.2.1 Skenario 1: Service HTTP <i>Allow</i>	22
IV.2.1.1 Pengujian Sebelum Serangan	23
IV.2.1.1.1 Data Hasil Pemantauan Sebelum Serangan	24
A. Data Hasil Berdasarkan Nilai CPU	24
B. Data Hasil Berdasarkan Nilai <i>Memory</i>	25

C.	Data Hasil pada <i>Bandwidth</i> Sebelum Serangan.....	27
D.	Data Hasil pada <i>Session</i> Sebelum Serangan.....	28
IV.2.1.2	Pengujian Saat Serangan	30
IV.2.1.2.1	Data hasil pemantauan Sumber Daya Komputasi Saat Serangan	31
A.	Data Hasil Berdasarkan Nilai CPU.....	32
B.	Data Hasil Berdasarkan Nilai <i>Memory</i>	33
C.	Data Hasil pada <i>Bandwidth</i> Saat Serangan.....	34
D.	Data Hasil pada <i>Session</i> Saat Serangan	36
IV.2.1.3	Pengujian Setelah Serangan	37
IV.2.1.3.1	Data Hasil Pemantauan Sumber Daya Komputasi Setelah Serangan	38
A.	Data hasil Berdasarkan Nilai CPU.....	39
B.	Data Hasil Berdasarkan Nilai <i>Memory</i>	40
C.	Data Hasil pada <i>Bandwidth</i> Setelah Serangan	41
D.	Data Hasil pada <i>Session</i> Setelah Serangan	43
IV.2.2	Skenario 2: Service HTTP <i>Block</i>	45
IV.2.2.1	Pengujian Sebelum Serangan	45
IV.2.2.1.1	Data Hasil Pemantauan Sebelum Serangan.....	47
A.	Data Hasil Berdasarkan Nilai CPU.....	47
B.	Data Hasil Berdasarkan Nilai <i>Memory</i>	48
C.	Data Hasil pada <i>Bandwidth</i> Sebelum Serangan.....	50
IV.2.2.2	Pengujian Saat Serangan	51
IV.2.2.2.1	Data hasil pemantauan Sumber Daya Komputasi Saat Serangan	53
A.	Data Hasil Berdasarkan Nilai CPU.....	53
B.	Data Hasil Berdasarkan Nilai <i>Memory</i>	54
C.	Data Hasil pada <i>Bandwidth</i> Saat Serangan.....	56
IV.2.2.3	Pengujian Setelah Serangan	57
IV.2.1.2.1	Data hasil pemantauan Sumber Daya Komputasi Setelah Serangan	58
A.	Data Hasil Berdasarkan Nilai CPU.....	59
B.	Data Hasil Berdasarkan Nilai <i>Memory</i>	60
C.	Data Hasil pada <i>Bandwidth</i> Setelah Serangan	61
BAB V	ANALISIS HASIL PENGUJIAN.....	64
V.1	Skenario 1: Analisis Pengujian <i>Service HTTP Allow</i>	64

V.1.1 Analisis Hasil Pengujian Sebelum Serangan.....	64
A. Analisis Sumber Daya Komputasi pada <i>CPU Usage</i>	64
B. Analisis Sumber Daya Komputasi pada <i>Memory Usage</i>	65
C. Analisis Sumber Daya Komputasi pada <i>Bandwidth</i>	72
D. Analisis Sumber Daya Komputasi pada <i>Session</i>	72
V.1.2 Analisis Hasil Pengujian Saat Serangan	75
A. Analisis Sumber Daya Komputasi pada <i>CPU Usage</i>	75
B. Analisis Sumber Daya Komputasi pada <i>Memory Usage</i>	82
C. Analisis Sumber Daya Komputasi pada <i>Bandwidth</i>	89
D. Analisis Sumber Daya Komputasi pada <i>Session</i>	91
V.1.3 Analisis Hasil Pengujian Setelah Serangan	94
A. Analisis Sumber Daya Komputasi pada <i>CPU Usage</i>	94
B. Analisis Sumber Daya Komputasi pada <i>Memory Usage</i>	101
C. Analisis Sumber Daya Komputasi pada <i>Bandwidth</i>	108
D. Analisis Sumber Daya Komputasi pada <i>Session</i>	111
V.2 Skenario 2: Analisis Pengujian Service HTTP Block	114
V.2.1 Analisis Hasil Pengujian Sebelum Serangan.....	114
A. Analisis Sumber Daya Komputasi pada <i>CPU Usage</i>	114
B. Analisis Sumber Daya Komputasi pada <i>Memory Usage</i>	121
C. Analisis Sumber Daya Komputasi pada <i>Bandwidth</i>	128
V.2.2 Analisis Hasil Pengujian Saat Serangan	131
A. Analisis Sumber Daya Komputasi pada <i>CPU Usage</i>	131
B. Analisis Sumber Daya Komputasi pada <i>Memory Usage</i>	138
C. Analisis Sumber Daya Komputasi pada <i>Bandwidth</i>	145
V.2.3 Analisis Hasil Pengujian Setelah Serangan	148
A. Analisis Sumber Daya Komputasi pada <i>CPU Usage</i>	148
B. Analisis Sumber Daya Komputasi pada <i>Memory Usage</i>	155
C. Analisis Sumber Daya Komputasi pada <i>Bandwidth</i>	162
V.3 Perbandingan Hasil Analisis Pengujian <i>Service HTTP Allow</i> dengan <i>Service HTTP Block</i>	165
A. Sebelum Serangan	165
B. Saat Serangan	166
1. Penggunaan <i>CPU Firewall</i>	167
2. Penggunaan <i>Memory Firewall</i>	169
C. Setelah Serangan.....	172
BAB VI KESIMPULAN DAN SARAN	173

VI. 1 Kesimpulan	173
VI. 2 Saran	173
DAFTAR PUSTAKA	174