

DAFTAR TABEL

Tabel 3.1 Perangkat Keras yang di Gunakan.....	17
Tabel 3.2 Perangkat Lunak yang di Gunakan.....	17
Tabel 3.3 Daftar Fungsi pada Sistem yang akan di terapkan.....	19
Tabel 3.4 <i>Use case description login</i>	22
Tabel 3.5 <i>Use case description logout</i>	22
Tabel 3.6 <i>Use case description issues</i>	23
Tabel 3.7 <i>Use case description view documentation</i>	23
Tabel 3.8 <i>Use case description calendar</i>	23
Tabel 3.9 <i>Use case description threats</i>	24
Tabel 3.10 <i>Use case description events</i>	24
Tabel 3.11 <i>Use case description severity</i>	24
Tabel 3.12 <i>Use case description sources</i>	25
Tabel 3.13 <i>Use case description trails</i>	25
Tabel 3.14 <i>Use case description view threats per page</i>	25
Tabel 3.15 <i>Use case description filter search</i>	26
Tabel 3.16 <i>Use case description clear</i>	26
Tabel 3.17 <i>Use case description print</i>	26
Tabel 3.18 <i>Use case description tools</i>	27
Tabel 4.1 Pengujian dengan Sejumlah Domain	37
Tabel 4.2 Metode Penerapan Serangan.....	37
Tabel 4.3 Hasil Pengujian Throughput <i>malware</i> sinkhole conficker	46
Tabel 4.4 Hasil Pengujian Throughput <i>malware</i> andromeda	46
Tabel 4.5 Hasil Pengujian Throughput <i>malware</i> sinkhole shadowserver	47
Tabel 4.6 Hasil Pengujian Throughput <i>malware</i> sinkhole response	47
Tabel 4.7 CPU <i>utilization</i> tanpa Maltrail dan Fail2Ban	51
Tabel 4.8 CPU <i>utilization</i> tanpa Maltrail dan Fail2Ban	51
Tabel 4.9 CPU <i>utilization</i> dengan serangan selain <i>malware</i>	51
Tabel 4.10 Hasil Pengukuran Throughput.....	52
Tabel 4.11 Hasil Analisis Pemantauan dan Pengamanan pada Server	52
Tabel 4.12 Hasil Uji Optimasi Sistem	53