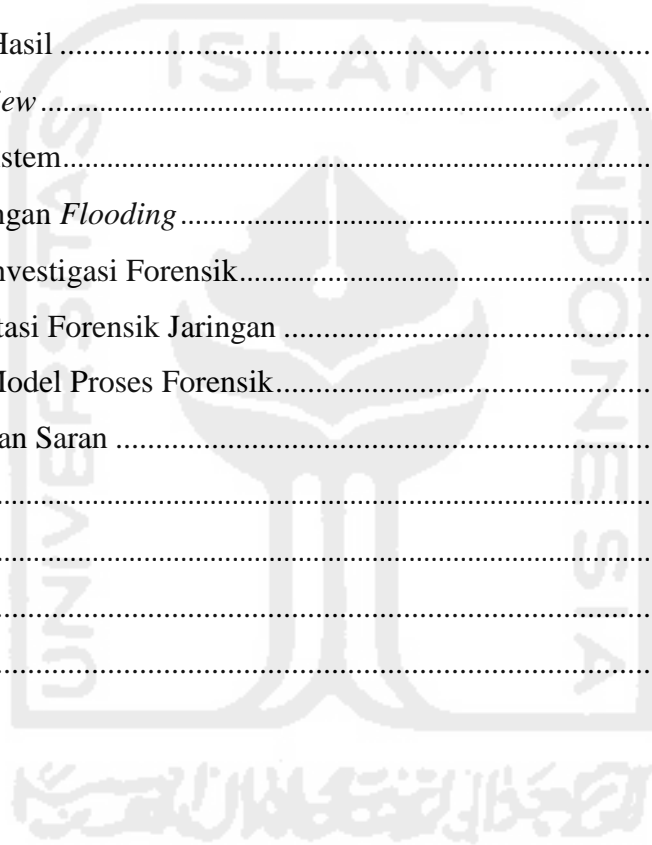


Daftar Isi

Abstrak	iv
Abstract	v
Pernyataan keaslian tulisan	vi
Publikasi selama masa studi	vii
Publikasi yang menjadi bagian dari tesis	vii
Kontribusi yang diberikan oleh pihak lain dalam tesis ini	viii
Kata Pengantar	x
Daftar Isi	xii
Daftar Gambar	xiv
Daftar Tabel	xvi
Bab 1 Pendahuluan	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	5
1.6 Review Penelitian	5
1.7 Metode Penelitian	11
1.8 Sistematika Penulisan	12
Bab 2 Landasan Teori	13
2.1 Forensik dan Forensik Jaringan	13
2.2 Model Proses <i>Forensic</i>	14
2.3 Komponen Jaringan	16
2.4 Serangan <i>Flooding</i>	17
2.5 <i>Intrusion Detection System (IDS)</i>	21
2.6 Snort	22
2.6.1 Komponen Snort	23
2.6.2 Aturan Snort	23
2.6.3 Kepala Aturan (<i>rule header</i>)	25
2.6.4 <i>Class Type</i>	25

2.6.5 Jenis Opsi <i>Rule</i>	26
2.6.6 Membaca Aturan Snort	27
Bab 3 Metodologi Penelitian	28
3.1 Literatur <i>Review</i>	28
3.2 Identifikasi Sistem	28
3.3 Konfigurasi Snort	29
3.4 Simulasi Kasus	30
3.5 Analisis	31
3.6 Laporan	33
Bab 4 Analisis dan Hasil	35
4.1 Literatur <i>Review</i>	35
4.2. Identifikasi Sistem	36
4.3 Simulasi Serangan <i>Flooding</i>	38
4.4 Analisis dan Investigasi Forensik	39
4.4.1 Implementasi Forensik Jaringan	40
4.4.2 Analisis Model Proses Forensik	41
Bab 5 Kesimpulan dan Saran	55
5.1 Kesimpulan	55
5.2 Saran	56
Daftar Pustaka	57
Lampiran	59



Daftar Gambar

<i>Gambar 1. 1 Top Network Attack</i>	1
<i>Gambar 1. 2 Statistik Flooding Attack</i>	3
<i>Gambar 1. 3 Metodologi Penelitian</i>	11
<i>Gambar 2. 1 Forensic Science</i>	13
<i>Gambar 2. 2 Turunan Ilmu Forensik</i>	14
<i>Gambar 2. 3 Serangan DoS</i>	17
<i>Gambar 2. 4 Serangan DDoS</i>	17
<i>Gambar 2. 5 SYN Flooding</i>	19
<i>Gambar 2. 6 Serangan ICMP</i>	20
<i>Gambar 2. 7 Serangan Peer-to-peer</i>	20
<i>Gambar 2. 8 Permanen DoS</i>	21
<i>Gambar 2. 9 Simple Snort Network Topology</i>	23
<i>Gambar 2. 10 Struktur Rule</i>	24
<i>Gambar 2. 11 Snort IDS rule header structure</i>	24
<i>Gambar 2. 12 Snort IDS Example</i>	24
<i>Gambar 2. 13 Blog Diagram</i>	27
<i>Gambar 3. 1 Alur Metodologi Penelitian</i>	28
<i>Gambar 3. 2 Tahapan Implementasi Intrusion Detection System (IDS) Snort</i>	29
<i>Gambar 3. 3 Prinsip Kerja Sistem Snort</i>	29
<i>Gambar 3. 4 Simulasi Kasus</i>	31
<i>Gambar 3. 5 Tahap simulasi serangan flooding pada web server</i>	31
<i>Gambar 3. 6 Model Proses Forensik</i>	33
<i>Gambar 3. 7 Tahapan penyusunan laporan</i>	34
<i>Gambar 4. 1 Proses autentifikasi server</i>	37
<i>Gambar 4. 2 Arsitektur Forensik Jaringan</i>	37
<i>Gambar 4. 3 Remote Server</i>	38
<i>Gambar 4. 4 Serangan Flooding</i>	39
<i>Gambar 4. 5 Topologi Jaringan UMMgl</i>	40
<i>Gambar 4. 6 Arsitektur Forensik jaringan</i>	40
<i>Gambar 4. 7 Proses Pengambilan Data</i>	42
<i>Gambar 4. 8 Alur Intrusion Detection System (IDS) Snort</i>	43
<i>Gambar 4. 9 Interface Trafik Intrusion Detection System (IDS) Snort</i>	46
<i>Gambar 4. 10 Traffic Normal</i>	47
<i>Gambar 4. 11 Trafik Serangan</i>	47
<i>Gambar 4. 12 Memory Usage</i>	48
<i>Gambar 4. 13 Memory Usage</i>	49

<i>Gambar 4. 14 logged In Users</i>	49
<i>Gambar 4. 15 Runing Processes</i>	50
<i>Gambar 4. 16 Filter ip.src</i>	50
<i>Gambar 4. 17 Follow UDP</i>	51
<i>Gambar 4. 18 Hasil follow UDP</i>	51
<i>Gambar 4. 19 Hasil frame</i>	52
<i>Gambar 4. 20 Statistik Endpoint Snort</i>	52



Daftar Tabel

<i>Tabel 1. 1 Tabel Literatur Review</i>	8
<i>Tabel 1. 2 Cont'd litelatur Review</i>	9
<i>Tabel 1. 3 Con't litelatur Review</i>	10
<i>Tabel 2. 1 Prioritas Klasifikasi Serangan</i>	25
<i>Tabel 2. 2 Con't Prioritas Klasifikasi Serangan</i>	26
<i>Tabel 3. 1 Pengelompokan Data</i>	33
<i>Tabel 4. 1 Prioritas Klasifikasi Serangan</i>	53
<i>Tabel 4. 2 Con't Prioritas Klasifikasi Serangan</i>	54

