

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
PERNYATAAN	iii
KATA PENGANTAR	iv
DAFTAR ISI	vi
DAFTAR TABEL	ix
DAFTAR GAMBAR	x
INTISARI	xii
ABSTRACT	xiii
BAB I 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 Keaslian Penelitian	5
1.7 Metodologi Penelitian	6
1.7.1 Metode Pengumpulan Data	6
1.7.2 Metode Pengembangan Sistem	6
1.8 Sistematika Penulisan	7
BAB II TINJAUAN PUSTAKA	9
BAB III LANDASAN TEORI	14
3.1 Jaringan Komputer	14
3.1.1 Konsep Komunikasi Jaringan	14
3.1.2 Jenis-Jenis Jaringan Komputer	15
3.2 Teori Keamanan Jaringan	15
3.2.1 Tujuan Keamanan Komputer	16
3.2.2 Aspek-Aspek Ancaman Keamanan Jaringan	17
3.3 Intrusion Detection System (IDS)	17
3.3.1 Jenis-Jenis IDS	19
3.3.2 Cara Kerja IDS	21
3.4 SNORT	23
3.4.1 Macam-Macam Mode	24
3.4.2 Komponen-Komponen Dasar Snort	25
3.4.3 Rule Snort	27
3.4.4 Proses Deteksi Snort	30
3.5 Aplikasi Pendukung Snort	30

3.5.1	Barnyard2	30
3.5.2	BASE (Basic Analysis and Security Engine)	31
3.6	Pengertian Port Number	32
3.6.1	Jenis Port Number	32
3.6.2	Teknik – Teknik Port Scanning	33
3.7	Jenis dan Teknik Serangan	34
3.7.1	Jenis-Jenis Serangan	35
3.7.2	Teknik Serangan dengan Port Scanning	36
3.8	Virtual Mesin	43
BAB IV ANALISIS PERANCANGAN		44
4.1	Analisis Sistem	44
4.2	Analisis Kebutuhan	45
4.2.1	Kebutuhan Fungsional Sistem	45
4.2.2	Kebutuhan non-Fungsional Sistem	45
4.3	Analisis Identifikasi Sistem	45
4.3.1	Kebutuhan Perangkat Keras	46
4.3.2	Kebutuhan Perangkat Lunak	46
4.3.3	Bahan	46
4.3.4	Sistem Pengujian dan Pengambilan Data	47
4.3.5	Analisis Alur Sistem	47
4.4	Design (Perancangan)	49
4.4.1	Perancangan Sistem	49
4.4.2	Perancangan Topologi Jaringan	50
4.5	Instalasi Software	50
4.5.1	Instalasi Snort	51
4.5.2	Instalasi Pulledpork	51
4.5.3	Instalasi Barnyard2	51
4.6	Perancangan Pembuatan Rule Snort	51
4.7	Sistem Pengujian	52
4.8	Analisis Sistem	52
BAB V IMPLEMENTASI		54
5.1	Deskripsi Implementasi Sistem	54
5.2	Lingkungan Penelitian	54
5.3	Konfigurasi Software	56
5.3.1	Konfigurasi MySQL	56
5.3.2	Konfigurasi Snort	57
5.3.3	Konfigurasi Barnyard2	59
5.3.4	Konfigurasi BASE	60
5.4	Konfigurasi Jaringan	60

5.5 Konfigurasi Snort Rules	61
BAB VI HASIL DAN PEMBAHASAN	62
6.1 Pengujian Sistem	62
6.1.1 Pengujian IP Scanning dan Port Scanning	62
6.1.2 Pengujian IDS dengan DoS	65
6.1.3 Pengujian IDS dengan SQL Injection	72
6.2 Analisis BASE (Base Analysis and Security Engine).....	74
6.2.1 Most Frequent 5 Unique Alert	75
6.2.2 IP Destination	76
6.2.3 Source TCP Protocol dan Numbers Alert.....	77
6.2.4 Destination TCP dan Alert	78
6.2.5 Source Protokol UDP	79
6.3 Hasil Pengujian Sistem	79
6.4 Kelebihan dan Kekurangan Sistem	80
6.4.1 Kelebihan Sistem	80
6.4.2 Kekurangan Sistem	81
BAB VII KESIMPULAN DAN SARAN.....	82
7.1 Kesimpulan	82
7.2 Saran.....	82
DAFTAR PUSTAKA	83