

DAFTAR ISI

HALAMAN PENGESAHAN	i
HALAMAN PERNYATAAN.....	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR GAMBAR	viii
DAFTAR TABEL	x
INTISARI	xi
ABSTRACT	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Metodologi Penelitian	4
1.7 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA	6
BAB III LANDASAN TEORI	13
3.1 Infrastruktur Jaringan	13
3.1.1 <i>Internet</i>	13
3.1.2 <i>Internet Service Provider (ISP)</i>	13
3.1.3 <i>Ping of Precences (PoP)</i>	13
3.1.4 <i>Network Access Point (NAP)</i>	14
3.1.5 <i>Local Area Network (LAN)</i>	14
3.1.6 <i>Network to Network</i>	14
3.2 Layanan <i>eGovernment</i>	15
3.3 Infrastruktur <i>eGovernment</i>	16
3.4 Keamanan Layanan <i>eGovernment</i>	17
3.5 Ancaman Keamanan Jaringan	18
3.5.1 Memaksa Masuk dan Kamus <i>Password</i>	18
3.5.2 <i>Denial of Service (DoS)</i>	18
3.5.3 <i>Spoofing</i>	20
3.5.4 Serangan <i>Man-in-the-middle</i>	20
3.5.5 <i>Spamming</i>	21
3.5.6 <i>Sniffer</i>	21
3.5.7 <i>Crackers</i>	21
3.6 <i>Intrusion Detection System (IDS)</i>	21
3.7 <i>Honeypot</i>	24
BAB IV ANALISIS DAN RANCANGAN SISTEM	27
4.1 Analisis Masalah	28
4.1.1 Sistem Pendeteksian Jaringan	28
4.1.2 Laporan Analisis Jaringan	28
4.1.3 <i>System Logging</i>	28

4.1.4	<i>Email Report Jaringan</i>	28
4.1.5	<i>Firewall</i>	29
4.1.6	Topologi Jaringan Saat Ini	29
4.1.7	Analisis SWOT	30
4.2	Analisis Kebutuhan Sistem	31
4.2.1	Analisis Kebutuhan Perangkat Keras	31
4.2.2	Analisis Kebutuhan Perangkat Lunak	31
4.3	Konsep Topologi Penelitian	32
4.4	Perancangan Skenario Pengujian	33
4.4.1	<i>Ping Flooding</i>	34
4.4.2	<i>Port Scanning</i>	35
4.4.3	<i>Distributed Denial of Service (DDoS)</i>	35
4.5	Analisis Hasil Pengujian	36
BAB V	IMPLEMENTASI	37
5.1	Instalasi <i>Snort</i>	37
5.1.1	Download <i>Snort</i>	37
5.1.2	Ekstrak <i>Snort</i>	38
5.1.3	Konfigurasi <i>Snort Startup</i>	39
5.1.4	Konfigurasi <i>Scrip Snort Startup</i>	40
5.2	Instalasi <i>Snort Rules</i>	42
5.2.1	Download <i>Snort Rules</i>	42
5.2.2	Ekstrak <i>Snort Rules</i>	42
5.2.3	Konfigurasi <i>Snort.conf</i>	43
5.2.4	Konfigurasi <i>Snort</i>	44
5.3	Implementasi <i>Snort IDS</i>	45
5.4	Instalasi <i>Barnyard2</i>	45
5.4.1	Download <i>Barnyard2</i>	46
5.4.2	Generate Paket <i>Barnyard2</i>	46
5.4.3	Konfigurasi <i>Startup Barnyard2</i>	47
5.5	Instalasi <i>Snorby</i>	49
5.5.1	Konfigurasi <i>Snorby</i>	49
5.5.2	Konfigurasi <i>Database Snorby</i>	50
5.5.3	Konfigurasi <i>Output Alert Barnyard2 ke Database Snorby</i>	52
5.5.4	Konfigurasi <i>Apache</i>	52
5.5.5	<i>Running Snorby</i>	53
5.6	Instalasi <i>Artillery Honeypot</i>	54
BAB VI	HASIL PENELITIAN DAN PEMBAHASAN	59
6.1	Pengujian <i>Ping Flooding</i>	59
6.2	Pengujian <i>Port Scanning</i>	61
6.3	Pengujian <i>Distributed Denial of Service (DDoS)</i>	62
6.4	Pendeteksian <i>Artillery</i>	63
6.5	Laporan Analisis Jaringan	64
6.6	<i>Email Report Jaringan</i>	67



BAB VII KESIMPULAN DAN SARAN	70
7.1 Kesimpulan	70
7.2 Saran	70
DAFTAR PUSTAKA	71
LAMPIRAN	73