

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	iii
PERNYATAAN BEBAS PLAGIASI	iv
KATA PENGANTAR	v
DAFTAR ISI	vi
DAFTAR GAMBAR	viii
DAFTAR TABEL	ix
INTISARI	x
ABSTRACT	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penelitian.....	3
BAB II TINJAUAN PUSTAKA	5
2.1 Jaringan Komputer	13
2.2 Keamanan Jaringan Komputer	14
2.3 <i>Intrusion Detection System (IDS)</i>	15
2.4 <i>Suricata</i>	16
2.5 <i>Snort</i>	18
2.6 <i>Rule</i>	20
2.7 <i>Barnyard2</i>	21
2.8 <i>Snorby</i>	22
2.9 <i>Pytnbull</i>	22
2.10 Hipotesis	24
BAB III BAHAN DAN METODE PENELITIAN	25
3.1 Bahan Penelitian	25
3.2 Peralatan Penelitian	25
3.3 Tahapan Penelitian	27



3.3.1	Perancangan Topologi	27
3.3.2	Perancangan <i>Wireless Router</i>	29
3.3.3	Implementasi <i>IDS Snort</i> pada <i>host Ubuntu Server</i>	30
3.3.4	Implementasi <i>IDS Suricata</i> pada <i>host Ubuntu Server</i>	34
3.3.5	Implementasi <i>tool</i> tambahan pada <i>host Ubuntu Server</i>	37
3.3.6	Implementasi <i>pytbull</i> pada <i>virtual BackTrack</i>	45
3.3.7	Skenario Pengujian	47
3.3.8	Pengujian Serangan	49
BAB IV HASIL PENELITIAN DAN PEMBAHASAN		54
4.1	Hasil Pengujian Serangan	54
4.1.1	Pengujian <i>Host Ubuntu Server</i> dengan <i>IDS Suricata</i>	55
4.2.2	Pengujian <i>Host Ubuntu Server</i> dengan <i>IDS Snort</i>	59
4.2	Hasil Jumlah Deteksi Serangan	62
4.3	Hasil Penggunaan <i>Resource</i> Sistem	64
4.4	Hasil Pengujian Kecepatan Deteksi.....	66
BAB V PENUTUP		71
5.1	Kesimpulan.....	71
5.2	Saran	71
DAFTAR PUSTAKA		72
LAMPIRAN		75

DAFTAR GAMBAR

Gambar 2.1 Topologi IDS Default	6
Gambar 2.2 Perbedaan Jaringan LAN, MAN dan WAN	14
Gambar 2.3 Penempatan NIDS dan HIDS pada jaringan.....	16
Gambar 3.1 Topologi Skenario Pengujian Suricata	27
Gambar 3.2 Topologi Skenario Pengujian Snort.....	28
Gambar 3.3 Tampilan alur kinerja deteksi	28
Gambar 3.4 Pengaturan Interface Setup WAN Wireless Router.....	29
Gambar 3.5 Pengaturan Jaringan Lokal Wireless Router.....	30
Gambar 3.6 Tampilan awal Snorby	44
Gambar 3.7 Tampilan Skenario Pengujian.....	48
Gambar 4.1 Tampilan pybull ketika menjalankan serangan	54
Gambar 4.2 Tampilan log deteksi dari IDS Suricata pada berkas log.....	55
Gambar 4.3 Log deteksi ids suricata pada database mysql server.....	56
Gambar 4.4 Tampilan deteksi event snorby ids suricata	57
Gambar 4.5 Tampilan informasi rules yang mendeteksi sebuah serangan.....	58
Gambar 4.6 Informasi log deteksi ids suricata pada snorby.....	58
Gambar 4.7 Tampilan log deteksi dari IDS Snort pada berkas log	59
Gambar 4.8 Log deteksi ids snort pada database mysql server	60
Gambar 4.9 Tampilan deteksi event snorby ids snort	60
Gambar 4.10 Tampilan informasi rules yang mendeteksi sebuah serangan.....	61
Gambar 4.11 Informasi log deteksi ids snort pada snorby	62
Gambar 4.12 Grafik sesi paket serangan yang berhasil terdeteksi dari kedua jenis IDS	63
Gambar 4.13 Grafik penggunaan resources memory sistem snort dan suricata ketika deteksi serangan.....	64
Gambar 4.14 Grafik penggunaan resources load cpu sistem snort dan suricata ketika deteksi serangan.....	65

DAFTAR TABEL

Tabel 2.1 Jumlah Serangan Setiap Modul	5
Tabel 2.2 Pengujian Tool Serangan.....	7
Tabel 2.3 Pengujian Parameter Serangan	8
Tabel 2.4 Indikator Pengujian	9
Tabel 2.5 Ringkasan Sumber Jurnal yang Telah Dilaksanakan	10
Tabel 3.1 Spesifikasi Laptop	25
Tabel 3.2 Spesifikasi Virtual Host Server	26
Tabel 3.3 Spesifikasi Virtual Backtrack	26
Tabel 3.4 Spesifikasi Wireless Router.....	26
Tabel 3.5 Modul dan Jumlah Serangan Pengujian	48
Tabel 4.1 Jumlah sesi paket serangan yang berhasil dideteksi kedua IDS.....	63
Tabel 4.2 Penggunaan Memory RAM dari IDS Snort dan IDS Suricata	64
Tabel 4.3 Persentase penggunaan load CPU dari IDS Snort dan IDS Suricata.....	65
Tabel 4.4 Kecepatan deteksi snort dan suricata pada serangan shellcodes	66
Tabel 4.5 Kecepatan deteksi ids snort dan ids suricata ketika serangan dos.....	67
Tabel 4.6 Jumlah log deteksi kedua ids untuk pengujian parameter count	68