

DAFTAR ISI

HALAMAN SAMPUL	i
LEMBAR PENGESAHAN	iii
PERNYATAAN BEBAS PLAGIASI.....	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL	x
INTISARI.....	xi
ABSTRACT.....	xii
BAB I	13
1.1 Latar Belakang.....	13
1.2 Rumusan Masalah	15
1.3 Batasan Masalah.....	16
1.4 Tujuan Penelitian.....	16
1.5 Manfaat Penelitian.....	17
1.6 Sistematika Penulisan.....	17
BAB II.....	19
2.1 Konsep Jaringan Komputer	19
2.2 Keamanan Jaringan Komputer	21
2.3 Serangan Pada Jaringan Komputer	21
2.4 Sistem Deteksi Intrusi (Intrusion Detection System)	23
2.5 Cara Kerja Intrusion Detection System	24
2.5.1 Signature Based Detection.....	24
2.5.2. Anomaly based detection	24
2.5.3 Stateful protocol analysis based	25
2.6 Jenis Area Kerja IDS	25
2.6.1 Host Intrusion Detection System (HIDS).	25
2.6.2 Network Intrusion Detection System (NIDS).....	26
2.7 Snort.....	27
2.8 Suricata.....	28
2.9 Pytbull.....	29
2.10 Raspberry Pi 3 Model B+	31
2.11 Rules	31
2.12 Referensi Penelitian Sebelumnya	31
2.13 Hipotesis	34
BAB III	35



3.1 Bahan.....	35
3.2 Peralatan	35
3.3 Prosedur Penelitian.....	37
3.4 Instalasi dan Konfigurasi Snort	40
3.5 Instalasi dan Konfigurasi Suricata.....	47
3.6 Instalasi Attacker Host Pytbull Pada Ubuntu 16.04	53
3.7 Skenario Pengujian.....	54
3.8 Pengujian Serangan	56
3.9 Analisis Hasil.....	59
BAB IV.....	60
4.1 Hasil Pengujian Serangan.....	60
4.1.1 Hasil Pengujian IDS Suricata	61
4.1.2 Hasil Pengujian IDS Snort.....	62
4.2 Hasil Pengambilan Data dan Analisis Perbandingan	63
4.2.1 Penggunaan <i>Resource Hardware</i> CPU	63
4.2.2 Penggunaan <i>Resource Hardware</i> RAM.....	65
4.2.3 Jumlah Serangan Yang Terdeteksi.....	66
4.1.3 Kecepatan Deteksi Serangan	67
BAB V	70
5.1 Kesimpulan.....	70
5.2 Saran	71
DAFTAR PUSTAKA	72
LAMPIRAN	74

DAFTAR GAMBAR

Gambar 2. 1 arsitektur NIDS HIDS.....	26
Gambar 2. 2 Arsitektur NIDS	26
Gambar 3. 1 Bagan Alir Metode Penelitian	37
Gambar 3. 2 Snort Sudah Terinstall Dengan Benar	42
Gambar 3. 3 Snort Sudah Dapat Berjalan Mendeteksi Gangguan	46
Gambar 3. 4 Suricata Sudah Dapat Berjalan Mendeteksi Gangguan	53
Gambar 3. 5 Skenario 1 IDS Snort.....	55
Gambar 3. 6 Skenario 2 IDS Suricata.....	56
Gambar 3. 7 Snort Berjalan Mendeteksi Serangan.....	57
Gambar 3. 8 Suricata Berjalan Mendeteksi Serangan	58
Gambar 3. 9 Pytbull Melakukan Serangan Pada IDS Suricata.....	59
Gambar 4. 1 Tampilan Pengujian Serangan Pytbull.....	60
Gambar 4. 2 log serangan DOS IDS Suricata	61
Gambar 4. 3 log serangan Bruteforce IDS Suricata	61
Gambar 4. 4 log serangan Shellcodes IDS Suricata	62
Gambar 4. 5 log serangan DOS IDS Snort.....	62
Gambar 4. 6 log serangan Shellcodes IDS Snort.....	62
Gambar 4. 7 Grafik Perbandingan Penggunaan Resource Hardware CPU	64
Gambar 4. 8 Grafik Rata-Rata Perbandingan Penggunaan Resource Hardware CPU	64
Gambar 4. 9 Grafik Perbandingan Penggunaan Resource Hardware RAM.....	65
Gambar 4. 10 Grafik Perbandingan Penggunaan Resource Hardware RAM.....	66
Gambar 4. 11 Grafik Perbandingan Jumlah Serangan Yang Terdeteksi	67
Gambar 4. 12 Grafik Perbandingan Kecepatan Serangan DOS	68
Gambar 4. 13 Grafik Perbandingan Kecepatan Deteksi dan Durasi Serangan Shellcodes .	69



DAFTAR TABEL

Tabel 3. 1 Spesifikasi PC Attacker	36
Tabel 3. 2 Spesifikasi IDS Suricata	36
Tabel 3. 3 Spesifikasi IDS Snort	36
Tabel 3. 4 File Konfigurasi Snort	43
Tabel 3. 5 File vsftpd.conf	45
Tabel 3. 6 File Konfigurasi Suricata.....	49
Tabel 3. 7 file vsftpd.conf suricata	52
Tabel 4. 1 Perbandingan Penggunaan Resource Hardware CPU	63
Tabel 4. 2 Perbandingan Penggunaan Resource Hardware RAM.....	65
Tabel 4. 3 Perbandingan Jumlah Serangan Yang Terdeteksi	66
Tabel 4. 4 Perbandingan Kecepatan Deteksi Serangan DOS	68
Tabel 4. 5 Perbandingan Kecepatan Deteksi Serangan ShellCodes.....	69