

ABSTRAK

SMK PGRI Kras Kediri mengalami gangguan jaringan saat pelaksanaan ujian sekolah akibat serangan DoS dan DDoS yang membanjiri lalu lintas data hingga *server* tidak dapat merespons dengan baik. Penelitian ini bertujuan untuk mengimplementasikan *Intrusion Prevention System* (IPS) Suricata sebagai solusi perlindungan jaringan terhadap serangan tersebut. Dengan metode NDLC, penelitian dilakukan melalui tahapan analisis, desain, simulasi, implementasi, dan pengujian. Hasil pengujian menunjukkan bahwa setelah penerapan IPS Suricata, terjadi peningkatan performa jaringan secara signifikan, baik dari sisi *throughput*, *packet drop rate*, *latency*, maupun penggunaan CPU dan RAM. Suricata terbukti mampu menyaring dan memblokir lalu lintas berbahaya secara *real-time* tanpa mengganggu trafik sah, sehingga jaringan tetap stabil dan aman selama serangan berlangsung. Implementasi ini menunjukkan bahwa IPS Suricata efektif dalam meningkatkan keamanan jaringan dan menjaga kelancaran aktivitas berbasis komputer di lingkungan sekolah.

Kata Kunci: Suricata, *Intrusion Prevention System*, Keamanan Jaringan, DoS, DDoS

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN	iii
ABSTRAK	iv
KATA PENGANTAR.....	v
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xii
DAFTAR TABEL	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	5
1.3 Batasan Masalah	5
1.4 Tujuan Penelitian	6
1.5 Manfaat Penelitian	6
BAB II TINJAUAN PUSTAKA.....	7
2.1 Studi Literatur	7
2.2 Tinjauan Teori.....	13
2.2.1 Keamanan Jaringan.....	13
2.2.2 Intrusion Prevention System (IPS)	15
2.2.3 Suricata	16
2.2.4 <i>VirtualBox</i>	17
2.2.5 <i>Firewall</i>	17

2.2.6 IPTables	18
2.2.7 Diagram Proses <i>Intrusion Prevention System</i> (IPS)	19
BAB III METODOLOGI PENELITIAN	20
3.1 Metode Penelitian	20
3.2 Tahapan Penelitian.....	21
3.2.1 <i>Analysis</i>	21
3.2.2 <i>Design</i>	21
3.2.3 Simulation Prototyping	24
3.2.4 <i>Implement</i>	24
3.2.5 Monitoring	24
3.2.6 Management.....	25
3.3 Pengumpulan Data	25
3.4 Teknik Pengambilan Data.....	27
3.5.1 Metode Pengukuran	28
3.5.2 Alat dan Teknik Pengukuran	32
3.5.3 Analisis Data.....	33
BAB IV HASIL DAN PEMBAHASAN	35
4.1 <i>Instalasi</i> dan Konfigurasi Suriacata.....	35
4.2 Pengamatan Performa Jaringan Awal.....	40
4.3 Pengamatan Jaringan Saat Terjadi Serangan Sebelum Suricata Aktif.....	44
4.4 Pengamatan Jaringan Saat Terjadi Serangan Sesudah Suricata Aktif.....	56

4.5 Analisis Hasil Pengamatan Jaringan.....	66
4.5.1 Throughput	67
4.5.2 Packet Drop Rate.....	68
4.5.3 <i>Latency</i>	69
4.5.4 CPU dan <i>Usage</i> RAM.....	71
4.5.5 Tabel Keberhasilan Suricata dalam Menangani Serangan	73
BAB V KESIMPULAN DAN SARAN.....	74
5.1 Kesimpulan	74
5.2 Saran	77
DAFTAR PUSTAKA.....	81
DAFTAR RIWAYAT HIDUP	86
DAFTAR LAMPIRAN	87

DAFTAR GAMBAR

Gambar 2.1 Proses Intrusion Prevention System.....	19
Gambar 3.1 Metode NDLC.....	20
Gambar 3.2 Desain Rancangan Keamanan Jaringan	22
Gambar 3.3 Desain Topologi Jaringan	23
Gambar 4.1. 1 <i>Update Repository</i>	35
Gambar 4.1. 2 <i>Install Suricata</i>	36
Gambar 4.1. 3 <i>Install Iptables</i>	37
Gambar 4.1. 4 Nonaktifkan Pada <i>Af-Packet</i>	38
Gambar 4.1. 5 Direktori <i>Custom Rules</i>	38
Gambar 4.1. 6 Integrasi <i>Iptbles</i> Ke NFQUEUE.....	39
Gambar 4.1. 7 Pembuat <i>Rules</i> Baru	40
Gambar 4.2. 1 Throughput Dalam Keadaan Normal	41
Gambar 4.2. 2 Packet Drop Rate Dalam Keadaan Normal.....	41
Gambar 4.2. 3 Latency Dalam Keadaan Normal	42
Gambar 4.2.4 CPU dan Usage RAM Dalam Keadaan Normal	43
Gambar 4.3. 1 Hasil Throughput saat Serangan Ping Flood tanpa Suricata Aktif	44
Gambar 4.3. 2 Hasil Packet Drop saat Serangan Ping Flood tanpa Suricata Aktif	45
Gambar 4.3.3 Hasil Latency saat Serangan Ping Flood tanpa Suricata Aktif	46

Gambar 4.3. 4 Hasil CPU dan RAM saat Serangan Ping Flood tanpa Suricata Aktif	47
Gambar 4.3. 5 Hasil Throughput saat Serangan HTTP Flood tanpa Suricata Aktif	48
Gambar 4.3. 6 Hasil Packet Drop saat Serangan HTTP Flood tanpa Suricata Aktif	48
Gambar 4.3. 7 Hasil Latency saat Serangan HTTP Flood tanpa Suricata Aktif	49
Gambar 4.3. 8 Hasil CPU dan RAM saat Serangan HTTP Flood tanpa Suricata Aktif	50
Gambar 4.3. 9 Hasil Throughput saat Serangan SYN Flood tanpa Suricata Aktif	51
Gambar 4.3. 10 Hasil Packet Drop saat Serangan SYN Flood tanpa Suricata Aktif	51
Gambar 4.3. 11 Hasil Latency saat Serangan SYN Flood tanpa Suricata Aktif	52
Gambar 4.3. 12 Hasil CPU dan RAM saat Serangan SYN Flood tanpa Suricata Aktif	53
Gambar 4.3. 13 IP Penyerang Ping Flood.....	54
Gambar 4.3. 14 IP Penyerang HTTP Flood	55
Gambar 4.3. 15 IP Penyerang SYN Flood	56
Gambar 4.4. 1 Hasil Throughput Saat Serangan Ping Flood Suricata Aktif	57
Gambar 4.4. 2 Hasil Packet Drop Saat Serangan Ping Flood Suricata Aktif	57

Gambar 4.4. 3 Hasil Latency Saat Serangan Ping Flood Suricata Aktif	58
Gambar 4.4. 4 Hasil CPU dan RAM Saat Serangan Ping Flood Suricata Aktif.....	59
Gambar 4.4. 5 Hasil Throughput Saat Serangan HTTP Flood Suricata Aktif.....	60
Gambar 4.4. 6 Hasil Packet Drop Saat Serangan HTTP Flood Suricata Aktif.....	60
Gambar 4.4. 7 Hasil Latency Saat Serangan HTTP Flood Suricata Aktif	61
Gambar 4.4. 8 Hasil CPU dan RAM Saat Serangan HTTP Flood Suricata Aktif.....	62
Gambar 4.4. 9 Hasil Throughput Saat Serangan Syn Flood Suricata Aktif	63
Gambar 4.4. 10 Hasil Packet Drop Saat Serangan Syn Flood Suricata Aktif	64
Gambar 4.4. 11 Hasil Latency Saat Serangan Syn Flood Suricata Aktif	64
Gambar 4.4. 12 Hasil CPU dan RAM Saat Serangan Syn Flood Suricata Aktif.....	65

DAFTAR TABEL

Tabel 2.1 Tabel Penelitian Terdahulu	10
Tabel 4.3.1 Pengamatan Jaringan Saat Terjadi Serangan	56
Tabel 4.4. 1 Pengamatan Jaringan Setelah Suricata Aktif	66
Tabel 4.5.1.1 Analisis Throughput.....	67
Tabel 4.5.2.1 Analisis Packet Drop Rate	69
Tabel 4.5.3.1 Analisa Latency	70
Tabel 4.5.4.1 Analisis CPU dan usage RAM.....	72
Tabel 4.5.5.1 Keberhasilan Suricata	73