BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Pengukuran Aktifitas Serangan

Hasil pengukuran aktifitas serangan terdiri dari penerapan metode yang digunakan dengan jumlah serangan yang terus ditambahkan. Setiap metode baik anomaly based, signature based, dan gabungan signature anomaly based akan diberikan jumlah serangan yang sama. Sehingga dapat terlihat dari jumlah serangan yang terdeteksi metode mana yang lebih baik dalam mendeteksi setiap serangan yang terjadi.

4.1.1 Hasil Pengujian Serangan Dengan Anomali Based

Pada tahapan pengujian metode anomali based digunakan beberapa serangan yang bersifat *anomaly based* (AB) yaitu *udp flood, icmp flood,* dan *smurf attack,* maupun bersifat *signature based* (SB) yaitu *syn attack, fin attack,* dan *malware* trojan. Berikut hasil pengujian dengan menggunakan metode anomaly based ditunjukan pada tabel IV-1:

Tabel IV-1 Hasil Pengujian Serangan Anomaly Based

Jenis Serangan	Hasil Deteksi	Sifat Serangan
UDP Flood	Terdeteksi	Anomali
ICMP Flood	Terdeteksi	Anomali
Syn Attack	Tidak Terdeteksi	Signature
Malware (Trojan)	Tidak terdeteksi	Signature
Fin Attack	Tidak Terdeteksi	Signature
Smurf attack	Terdeteksi	Anomali

Tabel IV-1 menunjukan hasil pengujian metode *Anomaly Based* dengan menggunakan beberapa serangan yaitu *udp flood, icmp flood, smurf attacksyn attack, fin attack, malware*. Hasil pengujian menunjukan metode *anomaly* hanya dapat mendeteksi serangan *udp flood, icmp flood,* dan *smurf attack.* Sedangkan, serangan *syn attack, fin attack,* dan *malware* tidak dapat terdeteksi.

4.1.2 Hasil Pengujian Serangan Dengan Signature Based

Pada tahapan pengujian dengan menggunakan metode signature based, digunakan beberapa gangguan yang bersifat *anomaly based* (AB) yaitu *udp flood, icmp flood,* dan *smurf attack,* maupun bersifat *signature based* (SB) yaitu *syn attack, fin attack,* dan *malware trojan*. Berikut hasil pengujian dengan menggunakan metode signature based :

Tabel IV-2 Hasil Pengujian Serangan Signature Based

Jenis Serangan	Hasil Deteksi	Sifat Serangan
UDP Flood	Tidak Terdeteksi	Anomali
ICMP Flood	Tidak Terdeteksi	Anomali
Syn Attack	Terdeteksi	Signature
Malware (Trojan)	Terdeteksi	Signature
Fin Attack	Terdeteksi	Signature
Smurf Attack	Tidak Terdeteksi	Anomali

Tabel IV-2 menunjukan hasil pengujian metode *Signature Based* dengan menggunakan beberapa serangan yaitu *udp flood, icmp flood, smurf attack, syn attack, fin attack,* dan *malware*. Hasil pengujian menunjukan metode *signature*

based hanya dapat mendeteksi serangan *syn attack, fin attack,* dan *malware*. Sedangkan, serangan *icmp flood, udp flood,* dan *smurf attack* tidak dapat terdeteksi.

4.1.3 Hasil Pengujian Serangan Dengan SAB IDS

Pada tahapan pengujian dengan menggunakan metode signature based, digunakan beberapa gangguan yang bersifat anomaly based (AB) yaitu *udp flood, icmp flood,* dan *smurf attack,* maupun bersifat signature based (SB) yaitu *syn attack, fin attack,* dan *malware Trojan*. Berikut hasil pengujian dengan menggunakan metode SAB IDS.

Tabel IV-3 Hasil Pengujian Serangan Signature Anomaly Based

Jenis Serangan	Hasil Deteksi	Sifat Serangan
UDP Flood	Terdeteksi	Anomali
ICMP Flood	Terdeteksi	Anomali
Syn Attack	Terdeteksi	Signature
Malware (Trojan)	Terdeteksi	Signature
Fin Attack	Terdeteksi	Signature
Smurf Attack	Terdeteksi	Anomali

Tabel IV-3 menunjukan hasil pengujian metode *Signature Anomaly Based* dengan menggunakan beberapa serangan yaitu *udp flood, icmp flood, smurf attack, syn attack, fin attack,* dan *malware*. Hasil pengujian menunjukan metode *signature anomaly based* (SAB) dapat mendeteksi seluruh serangan.

4.1.4 Hasil Pengukuran Jumlah Serangan Dengan Anomali Based

Pada pengukuran jumlah serangan digunakan bertujuan untuk melihat jumlah serangan yang terdeteksi dan persentase deteksi yang dihasilkan dengan menggunakan metode *Anomaly Based*. Jumlah serangan yang diberikan secara terus menerus yaitu jumlah serangan mulai dari 2000 serangan hingga 20000 serangan, dengan menggunakan interval sebesar 2000 dan dilakukan selama 15 menit. Berikut hasil pengukuran jumlah serangan yang terdeteksi dengan metode *Anomaly Based* ditunjukkan tabel IV-4.

Tabel IV-4 Hasil Jumlah Serangan Anomaly Based

Jumlah Serangan (dalam ribu)	**Jenis Serangan**	**Serangan Terdeteksi (dalam ribu)**	**True Positive (dalam ribu)**	**True Negative (dalam ribu)**	**Persentase Deteksi (dalam persen)**
2	ICMP Flood, UDP Flood, Smurf Attack, Fin Attack, Syn Attack, Dan Malware (Trojan).	0,765	0,765	1,235	38.25
4		1,367	1,367	2,633	34.18
6		1,854	1,854	4,146	30.90
8		2,469	2,469	5,531	30.86
10		2,481	2,481	7,519	24.81
12		2,447	2,447	9,553	20.39
14		2,4	2,4	11,6	17.14
16		2,433	2,433	13,567	15.21
18		2,402	2,402	15,598	13.34
20		2,493	2,493	17,507	12.47

Berdasarkan tabel IV-4 menunjukan kinerja dari metode *anomaly based* terhadap serangan yang diberikan yaitu *ICMP flood, UDP flood, Smurf Attack, fin attack, syn attack,* dan *malware.* Didapatkan hasil bahwa metode *anomaly* dapat mendeteksi serangan dengan nilai 12,47% sampai 38,25%, dengan tingkat true negatif yang cukup besar. Nilai true negatif yang cukup besar dalam setiap deteksi serangan menimbulkan risiko yang cukup besar yaitu dengan tingkat keamanan yang sangat rendah.

4.1.5 Hasil Pengukuran Jumlah Serangan Dengan Signature Based

Pada pengukuran jumlah serangan digunakan bertujuan untuk melihat jumlah serangan yang terdeteksi dan persentase deteksi yang dihasilkan dengan menggunakan metode *Signature Based*. Jumlah serangan yang diberikan secara terus menerus yaitu jumlah serangan mulai dari 2000 serangan hingga 20000 serangan, dengan menggunakan interval sebesar 2000 dan dilakukan selama 15 menit. Dalam setiap serangan yang dilakukan setiap interval serangan diberikan dengan kombinasi berbagai serangan mulai dari serangan *icmp flood, udp flood, smurf attack, syn attack, fin attack,* dan *malware* yang bersifat *trojan* malware. Selain itu terdapat hasil kategori deteksi baik yang bersifat *true positive* maupun *true negative.* Berikut hasil pengukuran jumlah serangan yang terdeteksi dengan metode *Signature Based* ditunjukkan tabel IV-5.

Tabel IV-5 Hasil Jumlah Serangan Signature Based

Jumlah Serangan (dalam ribu)	**Jenis Serangan**	**Serangan Terdeteksi (dalam ribu)**	**True Positive (dalam ribu)**	**True Negative (dalam ribu)**	**Persentase Deteksi (dalam persen)**
2	ICMP Flood, UDP Flood, Smurf Attack, Fin Attack, Syn Attack, Dan Malware (Trojan).	1,204	1,204	0,796	60,20
4		2,556	2,556	1,444	63,90
6		3,024	3,024	2,976	50,40
8		3,345	3,345	4,655	41,81
10		3,818	3,818	6,182	38,18
12		4,302	4,302	7,698	35,85
14		4,821	4,821	9,179	34,44
16		5,414	5,414	10,586	33,84
18		5,840	5,840	12,160	32,44
20		6,329	6,329	13,671	31,65

Berdasarkan tabel IV-5 menunjukan kinerja dari metode *signature based* terhadap serangan yang diberikan yaitu *ICMP flood, UDP flood, Smurf Attack, fin attack, syn attack,* dan *malware.* Didapatkan hasil bahwa metode *signature* dapat mendeteksi serangan dengan nilai 31,65% sampai 63,90%, dengan tingkat true negatif lebih kecil dibandingkan dengan metode *anomaly based*. Metode *signature* menghasilkan true positif yang lebih besar dibandingkan dengan metode *anomaly* menunjukan bahwa metode *signature* memiliki tingkat penanganan risiko yang lebih baik.

4.1.6 Hasil Pengukuran Jumlah Serangan Dengan SAB IDS

Pada pengukuran jumlah serangan bertujuan untuk melihat jumlah serangan yang terdeteksi dan persentase deteksi menggunakan metode *Signature Anomaly Based* (SAB). Jumlah serangan mulai dari 2000 serangan hingga 20000 serangan, dengan menggunakan interval sebesar 2000 dan dilakukan selama 15 menit. Berikut hasil pengukuran jumlah serangan yang terdeteksi dengan metode *Signature Anomaly Based* ditunjukkan tabel IV-6.

Tabel IV-6 Hasil Jumlah Serangan Signature Anomaly Based

Jumlah Serangan (dalam ribu)	**Jenis Serangan**	**Serangan Terdeteksi (dalam ribu)**	**True Positive (dalam ribu)**	**True Negative (dalam ribu)**	**Persentase Deteksi (dalam persen)**
2	ICMP Flood, UDP Flood, Smurf Attack, Fin Attack, Syn Attack, Dan Malware (Trojan).	1,786	1,786	0,214	89,30
4		3,902	3,902	0,98	97,55
6		4,427	4,427	1,573	73,78
8		5,003	5,003	2,997	62,54
10		5,369	5,369	4,631	53,69
12		6,651	6,651	5,349	55,43
14		7,333	7,333	6,667	52,38
16		7,735	7,735	8,265	48,34
18		8,258	8,258	9,742	45,88
20		8,743	8,743	11,257	43,72

Berdasarkan tabel IV-6 menunjukan kinerja dari metode *Signature Anomaly Based* (SAB) terhadap serangan yang diberikan yaitu *ICMP flood, UDP flood, Smurf Attack, fin attack, syn attack,* dan *malware.* Didapatkan hasil bahwa metode SAB dapat mendeteksi serangan dengan nilai 43,72% sampai 97,55%, dengan tingkat

true negatif yang kecil dibandingkan dengan metode *signature* atau *anomaly based*. Dengan nilai true positif yang besar menggunakan SAB menunjukan bahwa metode tersebut dapat mendeteksi lebih banyak serangan sedangkan hanya melewatkan sedikit serangan dengan nilai true negative yang kecil. Nilai true negative yang kecil menunjukan bahwa metode SAB dapat meminimalkan risiko yang terjadi sehingga memiliki tingkat keamanan yang cukup tinggi.

4.2 Hasil Pengukuran Uji Responsi

Pengukuran uji responsi digunakan untuk mengukur seberapa cepat setiap metode mendeteksi serangan. Hasil uji responsi dari setiap metode yang digunakan ditnjukkan dengan tabel IV-7 berikut :

Tabel IV-7 Hasil Uji Responsi IDS

Metode	Waktu Serangan	Waktu Deteksi	Waktu Responsi (detik)
Anomaly Based	13:26:25	13:26:32	7
Signature Based	13:31:10	13:31:19	9
SAB IDS	13:39:20	13:39:21	1

Berdasarkan tabel diatas, terlihat bahwa metode gabungan *signature anomaly based* (SAB) mempunyai waktu response yang lebih baik yaitu dengan respon waktu 1 detik dibandingkan dengan metode *anomaly based* atau *signature based* yang memiliki waktu responsi masing – masing 7 detik dan 9 detik.

4.3 Hasil Pengukuran Komputasi Sumber Daya

Pengukuran komputasi sumber daya digunakan untuk melihat berapa besar setiap metode menghabiskan setiap sumber daya yang ada dalam mendeteksi setiap serangan yang terjadi.

4.3.1 Hasil Pengukuran Komputasi Anomali Based

Pengukuran jumlah komputasi digunakan untuk mengetahui berapa persentase penggunaan sumber daya komputasi (processor dan memori) yang digunakan oleh metode *Anomaly Based* dalam mendeteksi serangan. Hasil pengukuran ditunjukkan tabel IV-8, sebagai berikut :

Tabel IV-8 Hasil Pengukuran Komputasi Anomaly Based

Jumlah Serangan (dalam ribu)	**Jenis Serangan**	**Penggunaan CPU (dalam persen)**	**Penggunaan Memori (dalam persen)**
2	ICMP Flood, UDP Flood, Smurf Attack, Fin Attack, Syn Attack, Dan Malware (Trojan).	34	59
4		35	59
6		42	60
8		53	60
10		55	60
12		60	60
14		65	60
16		65	60
18		68	60
20		75	60

Dari tabel IV-8, terlihat bahwa penggunaan sumber daya komputasi baik processor maupun memori yang digunakan metode *anomaly based* dalam mendeteksi serangan mengalami fluktuasi terutama penggunaan pada processor. Penggunaan memori metode *anomaly based* terlihat stabil dengan nilai yang hampir sama. Sedangkan penggunaan processor cenderung lebih besar dengan setiap kenaikan interval serangan hingga mencapai nilai 75 % penggunaan processor.

4.3.2 Hasil Pengujian Komputasi Signature Based

Pengukuran jumlah komputasi digunakan untuk mengetahui berapa persentase penggunaan sumber daya komputasi (processor dan memori) yang digunakan oleh metode *Signature Based* dalam mendeteksi serangan. Hasil pengukuran ditunjukkan tabel IV-9, sebagai berikut :

Tabel IV-9 Hasil Pengukuran Komputasi Signature Based

Jumlah Serangan (dalam ribu)	**Jenis Serangan**	**Penggunaan CPU (dalam persen)**	**Penggunaan Memori (dalam persen)**
2	ICMP Flood, UDP Flood, Smurf Attack, Fin Attack, Syn Attack, Dan Malware (Trojan).	38	51
4		39	51
6		40	57
8		46	59
10		55	60
12		56	60
14		67	61
16		69	62
18		69	62
20		69	62

Dari tabel IV-9, terlihat bahwa penggunaan sumber daya komputasi baik processor maupun memori yang digunakan oleh metode signature based dalam mendeteksi serangan mengalami nilai naik turun. Penggunaan memori pada metode signature based terlihat lebih besar dengan mencapai nilai 62%. Sedangkan penggunaan processor cenderung lebih besar dengan setiap kenaikan interval serangan hingga mencapai nilai 69 % penggunaan processor.

4.3.3 Hasil Pengujian Komputasi Signature Anomali Based (SAB)

Pengukuran jumlah komputasi digunakan untuk mengetahui berapa persentase penggunaan sumber daya komputasi (processor dan memori) yang digunakan oleh metode SAB dalam mendeteksi serangan. Hasil pengukuran ditunjukkan tabel IV-10, sebagai berikut :

Tabel IV-10 Hasil Pengukuran Sumber Daya Komputasi SAB

Jumlah Serangan (dalam ribu)	**Jenis Serangan**	**Penggunaan CPU (dalam persen)**	**Penggunaan Memori (dalam persen)**
2	ICMP Flood, UDP Flood, Smurf Attack, Fin Attack, Syn Attack, Dan Malware (Trojan).	49	56
4		55	56
6		70	57
8		72	57
10		73.5	58
12		74	58
14		74	58
16		75	59
18		82	59
20		85	60

Dari tabel IV-10, terlihat bahwa penggunaan sumber daya komputasi baik processor maupun memori yang digunakan oleh metode SAB dalam mendeteksi serangan mengalami nilai naik turun. Penggunaan memori pada metode SAB lebih stabil dibawah nilai 60%. Sedangkan penggunaan processor cenderung lebih besar dengan setiap kenaikan interval serangan hingga mencapai nilai 85 % penggunaan processor.

4.4 Analisis Data

Pada tahapan Analisa, dilakukan Analisa terhadap aktifitas serangan yang dilakukan terhadap metode yang digunakan, uji responsi, serta penggunaan sumber daya komputasi yang digunakan. Pengujian dilakukan sebanyak 10 kali pengujian dengan jumlah serangan yang dinaikan dengan setiap internal berjumlah 2000 serangan.

4.4.1 Aktifitas Serangan

Analisa aktifitas serangan dilakukan untuk mengetahui tingkat jumlah deteksi serangan dan persentase deteksi dari setiap metode yang digunakan. Dari hasil pengukuran setiap metode yang digunakan terhadap serangan yang dilakukan, disajikan perbandingan penggunaan metode baik *anomaly based*, *signature based*, dan penggabungan *signature anomaly based* terhadap jumlah serangan yang terdeteksi, tabel IV-11 menunjukan hasil perbandingan setiap metode terhadap deteksi aktifitas serangan yang terjadi pada sistemberikut tabel perbandingan persentase jumlah deteksi.

Tabel IV-11 Perbandingan Persentase Deteksi Metode IDS

Jumlah Serangan (dalam ribu)	**Jenis Serangan**	**Persentase Deteksi Metode (dalam persen)**		
		Anomaly Based	**Signature Based**	**Signature Anomaly Based**
2	ICMP Flood, UDP Flood, Smurf Attack, Fin Attack, Syn Attack, Dan Malware (Trojan).	38.25	60.20	89.30
4		34.18	63.90	97.55
6		30.90	50.40	73.78
8		30.86	41.81	62.54
10		24.81	38.18	53.69
12		20.39	35.85	55.43
14		17.14	34.44	52.38
16		15.21	33.84	48.34
18		13.34	32.44	45.88
20		12.47	31.65	43.72

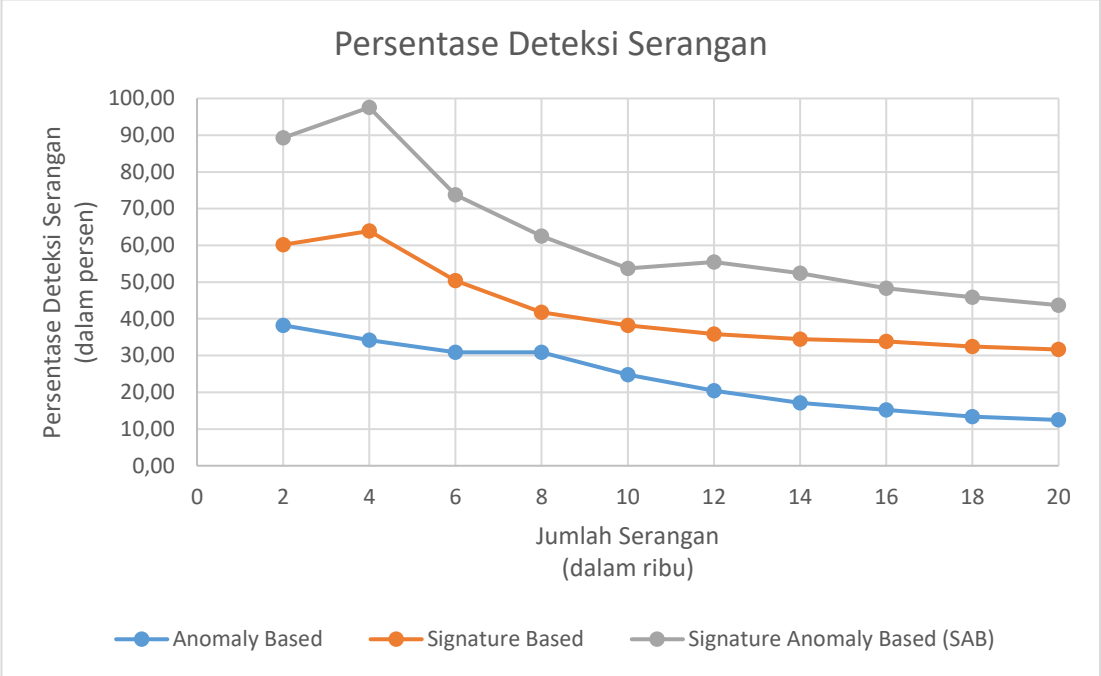
Pada tabel IV-11 diatas menunjukan persentase deteksi setiap metode IDS dalam mendeteksi serangan yang diberikan. Jumlah serangan yang diberikan secara terus menerus dari 2000 serangan dengan interval 2000 sampai jumlah serangan 20000.

Setiap serangan dinaikan setiap interval, perbandingan persentase jumlah deteksi setiap metode cenderung menurun dengan setiap kenaikan serangan. Metode SAB IDS menghasilkan persentase tertinggi dengan deteksi awal sebesar 89,30% dan terendah persentase deteksi sebesar 43,72%.

Tabel IV-12 Perbandingan Jumlah Deteksi Serangan Metode IDS

Jumlah Serangan (dalam ribu)	**Jenis Serangan**	**Jumlah Serangan Terdeteksi (dalam ribu)**		
		Anomaly Based	**Signature Based**	**Signature Anomaly Based**
2	ICMP Flood, UDP Flood, Smurf Attack, Fin Attack, Syn Attack, Dan Malware (Trojan).	0,765	1,204	1,786
4		1,367	2,556	3,902
6		1,854	3,024	4,427
8		2,469	3,345	5,003
10		2,481	3,818	5,369
12		2,447	4,302	6,651
14		2,400	4,821	7,333
16		2,433	5,414	7,735
18		2,402	5,840	8,258
20		2,493	6,329	8,743

Pada tabel IV-11 didapatkan data tentang perbandingan setiap metode dalam persentase deteksi setiap serangan yang terjadi. Untuk melihat setiap perbandingan serangan maka data tersebut disajikan dalam grafik perbandingan jumlah persentase deteksi setiap metode terhadap jumlah serangan yang dilakukan.



Gambar IV-1 Perbandingan Persentase Deteksi IDS

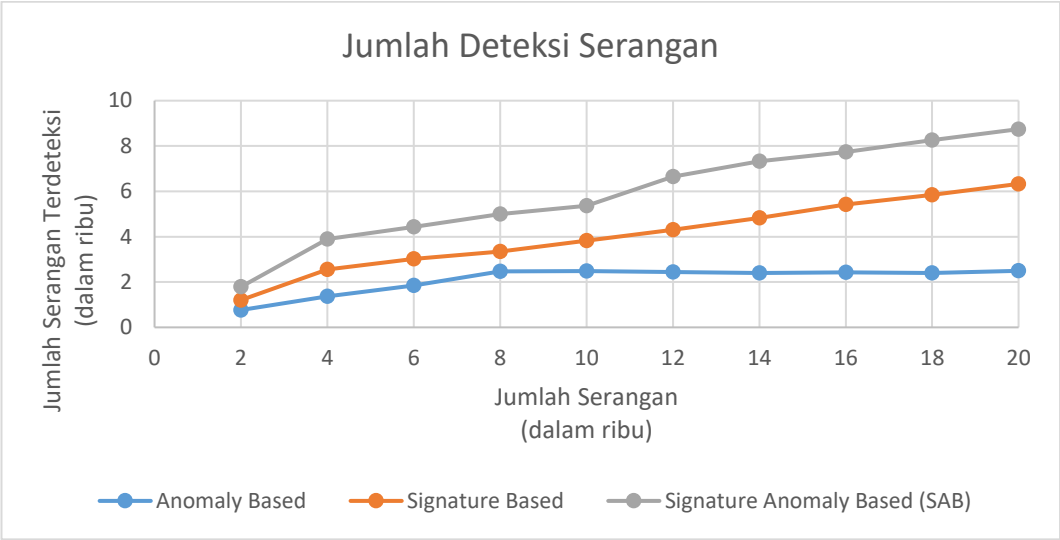
Pada grafik persentase deteksi metode IDS terhadap jumlah serangan didapatkan Analisa bahwa :

1. Metode anomali mendeteksi 2000 serangan awal sebesar 38,25%. Dengan kenaikan setiap jumlah serangan metode anomali dapat mendeteksi kurang dari 50% dengan terus menurun presentase deteksinya.

2. Metode signature mendeteksi 2000 serangan awal sebesar 60.20%. Dengan kenaikan setiap jumlah serangan metode signature dapat mendeteksi serangan dengan nilai yang terus berkurang tetapi masih dengan kisaran dibawah 35%.

3. Metode signature anomaly based mendeteksi 2000 serangan awal sebesar 89.30%.

Pada tabel IV – 12 didapatkan data tentang perbandingan jumlah deteksi serangan setiap metode. Untuk melihat setiap perbandingan deteksi serangan, maka disajikan grafik dibawah ini :



Gambar IV-2 Perbandingan Jumlah Deteksi IDS

Pada grafik jumlah serangan terdeteksi metode IDS terhadap jumlah serangan didapatkan Analisa bahwa :

1. Metode anomali dapat mendeteksi 2000 serangan awal dengan jumlah serangan terdeteksi sejumlah 765 *threat*.

2. Metode signature dapat mendeteksi 2000 serangan awal dengan jumlah serangan terdeteksi sejumlah 1204 *threat.*

3. Metode signature anomaly based dapat mendeteksi 2000 serangan awal dengan jumlah serangan terdeteksi sejumlah 1786 *threat*.

Dari ketiga metode dengan pengujian berbagai jumlah serangan, dapat terlihat bahwa metode gabungan signature anomaly based lebih baik dalam mendeteksi serangan dengan jumlah persentase deteksi tertinggi 97.55% dan terendah 43.72%.

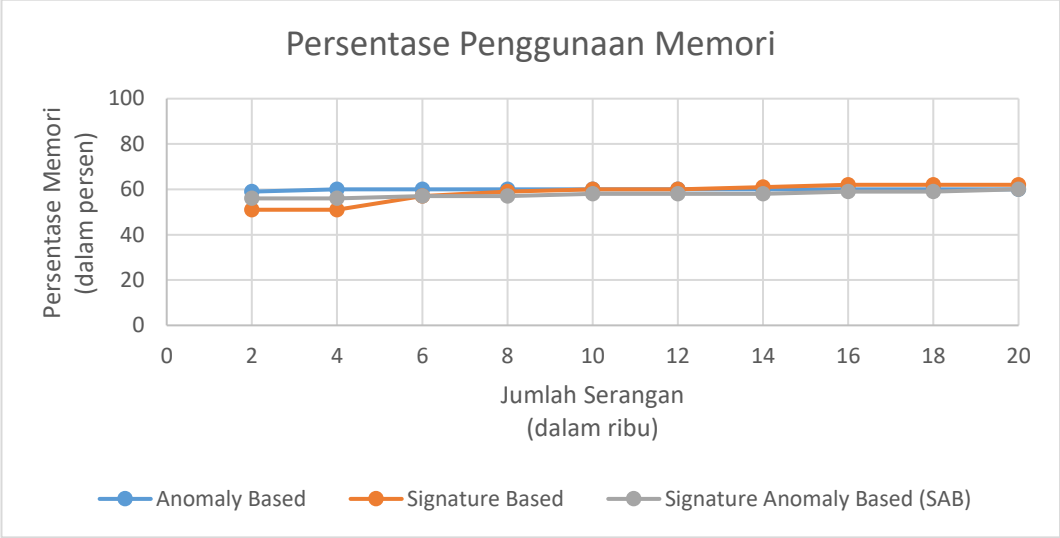
4.4.2 Penggunaan Memori

Dari hasil pengukuran setiap metode yang digunakan terhadap serangan yang dilakukan dapat disajikan perbandingan penggunaan metode baik *anomaly based*, *signature based*, serta penggabungan *signature anomaly based* terhadap penggunaan memori. Berikut tabel perbandingan persentase jumlah serangan terhadap penggunaan memori.

Tabel IV-13 Perbandingan Persentase Penggunaan Memori

Jumlah Serangan (dalam ribu)	**Jenis Serangan**	**Persentase Penggunaan Memori (dalam persen)**		
		Anomaly Based	**Signature Based**	**Signature Anomaly Based**
2	ICMP Flood, UDP Flood, Smurf Attack, Fin Attack, Syn Attack, Dan Malware (Trojan).	59	51	56
4		59	51	56
6		60	57	57
8		60	59	57
10		60	60	58
12		60	60	58
14		60	61	58
16		60	62	59
18		60	62	59
20		60	62	60

Pada tabel IV – 13 didapatkan data tentang perbandingan jumlah persentase penggunaan memori setiap metode. Untuk melihat setiap perbandingan penggunaan memori, maka disajikan grafik dibawah ini :



Gambar IV-3 Persentase Penggunaan Memori

Dari ketiga metode yang diterapkan dengan pengujian jumlah serangan, terlihat penggunaan memori setiap serangan cenderung lebih stabil dengan rata – rata persentase penggunaan memori yang sama. Pada serangan awal penggunaan memori metode gabungan signature anomaly based berada diantara metode anomaly dan signature based. Sedangkan penggunaan yang paling besar digunakan oleh metode anomaly based.

4.4.3 Penggunaan Processor (CPU)

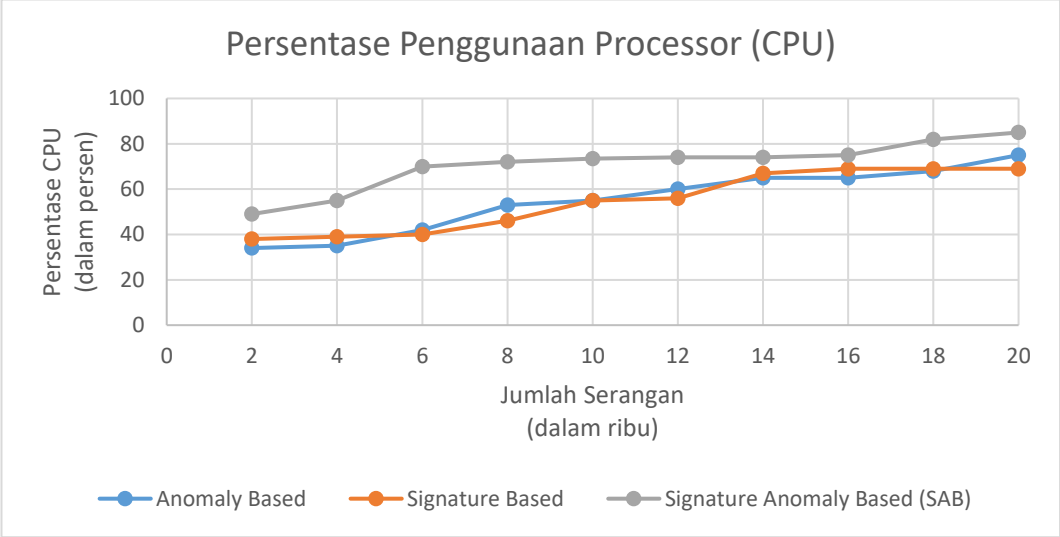
Dari hasil pengukuran setiap metode yang digunakan terhadap serangan yang dilakukan, disajikan perbandingan penggunaan metode anomaly based,

signature based, serta penggabungan signature anomaly based terhadap penggunaan processor (CPU).

Tabel IV-14 Perbandingan Persentase Penggunaan CPU (Processor)

Jumlah Serangan (dalam ribu)	**Jenis Serangan**	**Persentase Penggunaan CPU (dalam persen)**		
		Anomaly Based	**Signature Based**	**Signature Anomaly Based**
2	ICMP Flood, UDP Flood, Smurf Attack, Fin Attack, Syn Attack, Dan Malware (Trojan).	34	38	49
4		35	39	55
6		42	40	70
8		53	46	72
10		55	55	73.5
12		60	56	74
14		65	67	74
16		65	69	75
18		68	69	82
20		75	69	85

Pada tabel IV – 14 didapatkan data tentang perbandingan jumlah persentase penggunaan processor (CPU) setiap metode. Untuk melihat setiap perbandingan penggunaan processor, maka disajikan grafik dibawah ini :



Gambar IV-4 Persentase Penggunaan CPU

Dari ketiga metode yang diterapkan dengan pengujian berbagai jumlah serangan, dapat terlihat bahwa penggunaan processor setiap serangan cenderung terdapat perbedaan yang cukup besar. Pada 2000 serangan awal penggunaan processor dengan metode gabungan signature anomaly based cenderung mengkonsumsi penggunaan processor yang paling tinggi dibandingkan dengan metode yang lain yang hanya mengkonsumsi penggunaan processor yang lebih sedikit.

4.4.4 Analisa Tingkat Error

Untuk mengetahui tingkat error yang dihasilkan setiap metode digunakan penghitungan *Root Mean Square Error* (RMSE). Dengan menggunakan RMSE dapat dihitung tingkat kesalahan deteksi setiap metode IDS yang diberikan. Perhitungan RMSE menggunakan rumus :

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(Yi-\acute{Y}i)2}{n}} \quad \text{..... IV-1}$$

Keterangan :

Yi = Data Awal (Data Sebenarnya)

Ýi = Data Akhir (Data Percobaan)

n = Jumlah Percobaan

Tabel IV-15 Perhitungan RMSE

No.	**Yi (dalam ribu)**	**Anomali Based (dalam ribu)**			**Signature Based (dalam ribu)**			**Signature Anomali Based (dalam ribu)**		
		Ý	**Yi – Ýi**	**(Yi – Ýi)²**	**Ý**	**Yi – Ýi**	**(Yi – Ýi)²**	**Ý**	**Yi – Ýi**	**(Yi – Ýi)²**
1.	2	0,77	1,24	1,53	1,20	0,80	0,63	1,79	0,21	0,05
2.	4	1,37	2,63	6,93	2,56	1,44	2,09	3,90	0,10	0,01
3.	6	1,85	4,15	17,19	3,02	2,98	8,86	4,43	1,57	2,47
4.	8	2,47	5,53	30,59	3,35	4,66	21,67	5,00	3,00	8,98
5.	1	2,48	7,52	56,54	3,82	6,18	38,22	5,37	4,63	21,45
6.	12	2,45	9,55	91,26	4,30	7,70	59,26	6,65	5,35	28,61
7.	14	2,40	11,60	134,56	4,82	9,18	84,25	7,33	6,67	44,45
8.	16	2,43	13,57	184,06	5,41	10,59	112,06	7,74	8,27	68,31
9.	18	2,40	15,60	243,30	5,84	12,16	147,87	8,26	9,74	94,91
10.	20	2,49	17,51	306,50	6,33	13,67	186,90	8,74	11,26	126,72
Nilai RMSE				1072,45			661,80			395,96

Perhitungan RMSE untuk metode Anomali Based :

$$\text{RMSE} = \sqrt{\frac{\sum_{i=1}^{n}(Yi-Ýi)2}{n}}$$

$$\text{RMSE} = \sqrt{\frac{1072,45}{10}}$$

RMSE = $\sqrt{107,25}$

RMSE = 10,36

Pehitungan RMSE untuk metode Signature Based :

RMSE = $\sqrt{\frac{\sum_{i=1}^{n}(Yi-\acute{Y}i)2}{n}}$

RMSE = $\sqrt{\frac{661,80}{10}}$

RMSE = $\sqrt{66,18}$

RMSE = 8,14

Perhitungan RMSE untuk metode Signature Anomali Based (SAB) :

RMSE = $\sqrt{\frac{\sum_{i=1}^{n}(Yi-\acute{Y}i)2}{n}}$

RMSE = $\sqrt{\frac{395,96}{10}}$

RMSE = $\sqrt{39,60}$

RMSE = 6,29

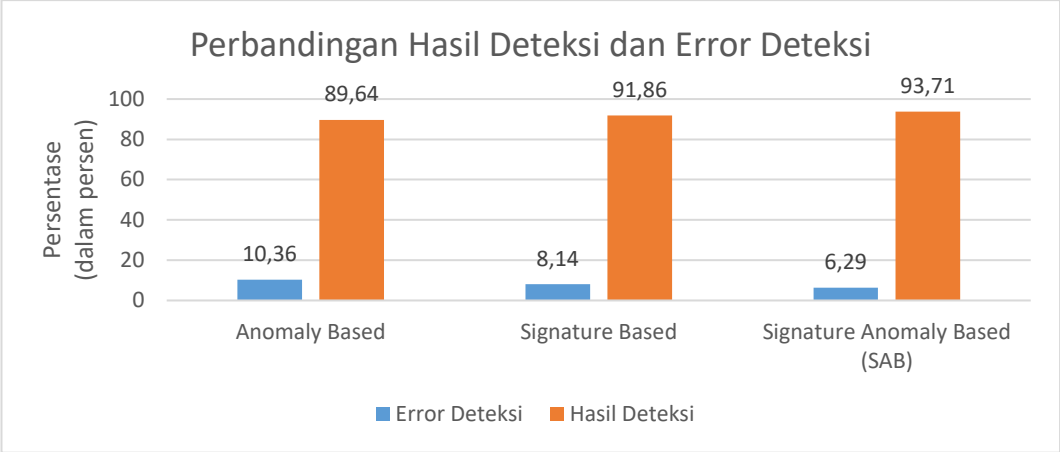
Perbandingan nilai RMSE setiap metode yang digunakan adalah :

Tabel IV-16 Perbandingan Nilai RMSE

Nilai RMSE		
Anomaly Based	**Signature Based**	**Signature Anomaly Based**
10,36	8,14	6,29

Tabel IV-16 menunjukan Analisa tingkat error setiap metode IDS dengan menggunakan Analisa nilai RMSE. Didapatkan hasil bahwa metode *anomaly based* memiliki nilai RMSE 10,36, sedangkan metode *signature* memiliki nilai 8,14, dan metode *Signature Anomaly Based* (SAB) memiliki nilai 6,29.

Berikut grafik perbandingan nilai tingkat error dan persentase deteksi setiap metode yang digunakan.



Gambar IV-5 Perbandingan Hasil Deteksi dan Error Deteksi

Dari perbandingan nilai tingkat error dengan menggunakan persamaan RMSE (*Root Mean Square Error*) didapatkan hasil :

1. Metode *Anomaly Based* memiliki tingkat keberhasilan deteksi 89,64 % dan tingkat error deteksi 10,36 %.
2. Metode *Signature Based* memiliki tingkat keberhasilan deteksi 91,86 % dan tingkat error deteksi 8,14 %.
3. Metode *Signature Anomaly Based* (SAB) memiliki tingkat keberhasilan deteksi 93,71 % dan tingkat error deteksi 6,29 %.