



**seminar nasional  
informatika 2017**



# PROSIDING

**"e-Defense : Menjaga keamanan data  
menghadapi cyber warfare untuk memperkuat  
kedaulatan Negara Kesatuan Republik Indonesia"**



**eDefense**  
seminar nasional informatika 2017



**ISSN 1979-2328**

**Yogyakarta, 25 November 2017**

## SUSUNAN PANITIA

**Penanggung Jawab** : Dekan Fakultas Teknik Industri  
**Pengarah** : 1. Wakil Dekan I FTI  
2. Wakil Dekan II FTI  
**Ketua Umum** : Ketua Program Studi Teknik Informatika  
**Wakil Ketua Umum** : Sekretaris Program Studi Teknik Informatika  
**Ketua Pelaksana** : Frans Richard Kodong, S.T., M.Kom.

**Reviewer** :

Assoc. Prof. Dr. Anton Satria Prabuwo, KSU  
Dr. Tech. Ahmad Azhari UGM  
Dr. Ir. Lukito Edi Nugroho, MT. UGM  
Dr. Ashari SN, UGM  
Ir. Balza Ahmad, M.Eng. UGM  
Joko Siswantoro, Universitas Surabaya  
Dr. Djoko Budianto, Atmajaya Yogyakarta  
Dr. Slamet, Universitas Muhammadiyah Malang, Indonesia.  
Dr. Abdul Kadir, STMIK Kartika Yani  
Nuryono Setyo Widodo, S.T., M.T., Universitas Ahmad Dahlan  
Dr. Herlina Jayadianti, S.T., M.T., UPN "Veteran" Yogyakarta  
Hafsah, S.T., M.T., UPN "Veteran" Yogyakarta  
Hidayatullah Himawan, S.T., M.M., M.Eng., UPN "Veteran" Yogyakarta  
Bambang Yuwono, S.T., M.T., UPN "Veteran" Yogyakarta

**Komite Pelaksana (Informatika UPN) :**

Agus Sasmito Aribowo, S.Kom., M.Cs  
Budi Santosa, S.Si., M.T.  
Dessyanto Boedi P, S.T., M.T.  
Frans Richard Kodong, S.T., M.Kom  
Herry Sofyan, S.T., M.Kom.  
Heriyanto, A.Md, S.Kom, M.Cs  
Heru Cahya Rustamadji, S.Si., M.T.  
Juwairiah, S.Si., M.T.  
Mangaras Yanu Florestiyanto, S.T., M.Eng  
Nur Heri Cahyana, S.T., M.Kom.  
Oliver Samuel Simanjuntak, S.Kom, M.Eng  
Paryati, S.T., M.Kom.  
Rifki Indra Perwira, S.Kom., M.Eng  
Simon Pulung Nugroho, S.T.  
Wilis Kaswidjanti, S.Si., M.Kom  
Yuli Fauziah, S.T., M.T.  
Budi Cahyono  
Pri Wahyu Eko Setiawan  
Rahayu Ari Orbani.  
Sugeng Rahmadi  
Sukardi  
Himpunan Mahasiswa Teknik Informatika (HIMATIF)

## DAFTAR ISI

<b>HALAMAN JUDUL</b>		<b>i</b>
<b>KATA PENGANTAR</b>		<b>iii</b>
<b>SUSUNAN PANITIA</b>		<b>iv</b>
<b>DAFTAR ISI</b>		<b>v</b>
<b>1 SISTEM PAKAR BERBASIS WEB MENGGUNAKAN TEOREMA BAYES (STUDI KASUS PENYAKIT SAAT BANJIR DI CIREBON)</b>	<i>Bambang Yuwono, Hidayatulah Himawan, Adi Yusuf</i>	<b>1</b>
<b>2 SISTEM INFORMASI GEOGRAFIS KOMANDO RAYON MILITER (KORAMIL) DAN KECAMATAN BINAAN KORAMIL DI KOTA YOGYAKARTA</b>	<i>Budi Santosa, Sri Rahayu Astari, Wilis Kaswidjanti</i>	<b>13</b>
<b>3 ANALISIS SISTEM MANAJEMEN KEAMANAN INFORMASI ELECTRONIC SECURITY SYSTEM (ESS) MENGGUNAKAN STANDAR ISO 27001 STUDI KASUS KANTOR PERWAKILAN BANK INDONESIA PROVINSI BALI</b>	<i>I Gede Putu Krisna Juliharta, I Made Maha Primananda Budi, I Gusti Agung Lanang Agung Raditya</i>	<b>19</b>
<b>4 IMPLEMENTASI DAN ANALISA BISNIS RENTAL WEB SYSTEM (SEWALOKA.COM) DENGAN PENDEKATAN SOFTWARE ARCHITECTURAL PATTERN MODEL-VIEW-CONTROLLER</b>	<i>I Putu Satwika, I Made Agus Apriliawan</i>	<b>26</b>
<b>5 REKAYASA SISTEM PENERIMA BEASISWA MISKIN DENGAN METODE C4.5 DAN ELECTRE</b>	<i>Made Henny Aryani, Rukmi Sari Hartati , Ni Wayan Sri Ariyani</i>	<b>37</b>
<b>6 APLIKASI SINGLE ACCOUNT BERBASIS WEB SERVICE MENGGUNAKAN AUTHETICATION LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)</b>	<i>Rifki Indra Perwira, Heru Cahya Rustamaji, Hendra Arya Syaputra</i>	<b>42</b>
<b>7 IMPLEMENTASI MAPPING OTOMATIS DARI DATABASE MYSQL 5.6 KE PROTEGE 4.3 DENGAN TURTLE ONTOLOGY, D2RQ, JENA, DAN NETBEANS 7.4</b>	<i>Widiatminingsih, Herlina jayadianti , Heru cahya Rustamaji</i>	<b>53</b>
<b>8 IMPLEMENTASI SISTEM PENGONTROLAN STOK BAHAN BAKU DAN BARANG JADI PADA GUDANG TEH</b>	<i>Wilis Kaswidjanti, Frans Ricard Kodong, Heru Tricahyono</i>	<b>64</b>
<b>9 KOMPARASI METODE DSS UNTUK MENENTUKAN PRIORITAS PROYEK PEMBANGUNAN DAERAH</b>	<i>Maya Marselia, Fathushahib</i>	<b>70</b>
<b>10 SURVEI PADA PENGGUNAAN TEKNIK DATA MINING PADA BIDANG KESEHATAN DI INDONESIA</b>	<i>Siti Khomsah</i>	<b>82</b>
<b>11 ANALISIS KEAMANAN SISTEM INFORMASI AKADEMIK UIN SUNAN KALIJAGA</b>	<i>Aries Firmansyah, Bambang Sugiantoro</i>	<b>91</b>

- |           |  |   |            |
|-----------|--|---|------------|
| <b>12</b> | <b>PERANCANGAN MALWARE LOCAL DAN ANTI-MALWARE MEMANFAATKAN SCRIPT BATCH FILE PADA PLATFORM WINDOWS DENGAN METODE FORWARD CHAIN</b> | <i>Frans Richard, Jefri<br/>Hutama Arbi</i>   | <b>100</b> |
| <b>13</b> | <b>REPRESENTASI BUDAYA YOGYAKARTA PADA DESAIN KAOS MENGGUNAKAN TEKNOLOGI AUGMENTED REALITY BERBASIS ANDROID</b>                    | <i>OliverSamuel<br/>Simanjunt, Hidayatullah<br/>Himawan<sup>1</sup>, Reza<br/>Raditya Setyo Putra</i> | <b>110</b> |

## ANALISIS KEAMANAN SISTEM INFORMASI AKADEMIK UIN SUNAN KALIJAGA

**Aries Firmansyah<sup>(2)</sup>, Bambang Sugiantoro<sup>(1)</sup>,**  
Teknik Informatika UIN Sunan Kalijaga  
Alamat Jl Marsda Adisucipto Yogyakarta  
e-mail : informatika@uin-suka.ac.id

### Abstract

*The Academic Information System is designed to support what you want users completed, the operating system must support the network to a certain extent. Therefore the need to be analysed performance computer network on information systems academic UIN Sunan Kalijaga Yogyakarta later the analysis can be used for development in the future. Testing tissue using a performance QoS (Quality of Service) and testing attacks have DDOS.*

*Research phase based on the quantitative method as the data collection to knowing how big performance of the academic information system to DDOS attack, scenario using big packet sent and conducted performance analysis of performance of the Academic Information System of UIN Sunan Kalijaga Yogyakarta emphasizes on monitoring of system and bandwidth parameters measurement, delay and packet loss on the network infrastructure that has been there is.*

*The result of measurement and monitoring Quality of Service on Academic Information System of UIN Sunan Kalijaga toward the Distributed Denial of Service attack (DDoS) decreased by the highest average score of bandwidth transfer rate 2.4 KBps what happened in the 1 PC attack and 10.1 KBps what happened in 2 PC attack. According to THIPON version, delay parameters indicated the average score of delay is bigger than 450 ms what happened in 1 PC attack by score 928.3 ms and 2 PC score 880.6 ms included in bad category. Meanwhile on packet loss parameters of 1 PC attack score 50.5 % and 2 PC score 82.2 % included in bad category that is by packet loss ranges more than 25 %.*

*Keyword: DDOS (Distributed Denial of Service), QoS (Quality of Service), Bandwidth, Delay, Packet Loss*

### Abstrak

*Pengukuran dan monitoring Quality of Service pada Sistem Informasi Akademik UIN Sunan Kalijaga terhadap serangan Distributed Denial of Service menurun dengan nilai rata-rata tertinggi bandwidth transfer rate sebesar 2.4 KBps yang terjadi di serangan 1 PC dan 10.1 KBps yang terjadi di serangan 2 PC. Menurut versi THIPON, parameter delay menunjukkan rata-rata nilai delay berkisar lebih besar dari 450 ms yang terjadi pada serangan 1 PC dengan nilai 928.3 ms dan 2 PC dengan nilai 880.6 ms termasuk dalam kategori Jelek. Sedangkan pada parameter packet loss pada serangan 1 PC dengan nilai 50.5% dan 2 PC dengan nilai 82.2% juga dalam kategori jelek yaitu dengan nilai packet loss-nya berkisar lebih dari 25%.*

*Berdasarkan penelitian hasil analisis Quality of Service dengan pengujian serangan Distributed Denial of Service dalam performa hardware bahwa jika serangan tidak banyak looping atau perulangan maka akan berpengaruh kepada RAM dan jika serangan banyak menggunakan looping atau perulangan akan berpengaruh kepada CPU.*

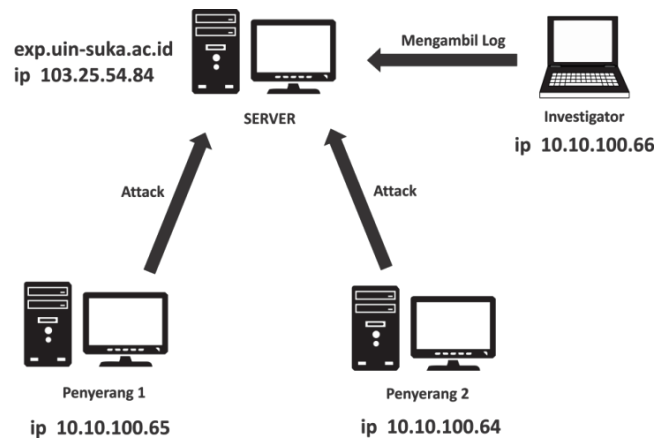
## 1. PENDAHULUAN

Menurut data keamanan IDSIRTII - Kemenkominfo insiden keamanan yang telah direkam dari pada tahun 2016, mereka mencatat 33,1% tidak diketahui asalnya, 15,1% serangan dari Account Hijacking, 11,6% dari Targeted Attack, 11,3% dari DDOS, 8,4% dari SQL Injection, 8,0% dari Malware, 4,9% dari Defacement, 1,8 % dari Malicious Iframe / JS, 0,4% dari DNS Hijacking, 0 % dari XSS, dan 6,0% dari Other Selain itu data keamanan IDSIRTII - Kemenkominfo juga mencatat dari hasil total jumlah serangan dengan jumlah 135.672.984 serangan, sektor mana saja yang diserang yaitu : Port paling banyak di serangan Port 53 , Jumlah total informasi celah keamanan 37.124 , 47% jumlah aktivasi malware 63.766303 , domain website paling banyak di serang .ac.id , 13.218 jumlah total insiden website. Salah satu penunjang vital pada perguruan tinggi adalah layanan sistem informasi akademik yang mempunyai mekanisme prosedur keamanan data yang baik sehingga perlu adanya standar keamanan sistem informasi yang baik untuk mendukung tercapainya pelayanan akademik yang baik. Salah satu perguruan tinggi yang menggunakan Teknologi Informasi di Yogyakarta adalah Universitas Islam Negeri

Sunan Kalijaga Yogyakarta. UIN menggunakan teknologi informasi sebagai sarana untuk memberikan informasi akademik kepada seluruh civitas akademika dan membantu terlaksananya kegiatan unit kerja yang ada.

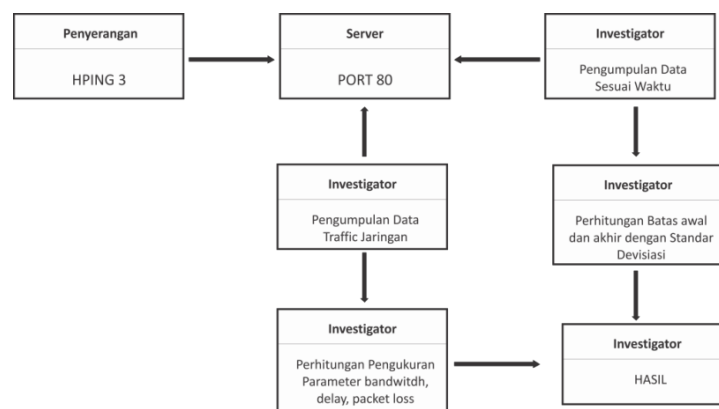
## 2. Metode Penelitian

Skenario penelitian bias diurai dalam bentuk gambar sebagai berikut :



Gambar 1 skenario serangan traffic jaringan terhadap serangan dan pengukuran kinerja Quality of Service (QoS).

Diagram aktifitas penelitian ini dapat dilihat pada gambar 2



Gambar 2 Diagram Aktifitas

Pada gambar 2 dapat dilihat topologi serangan dari penelitian ini melakukan serangan ke server kemudian pengambilan log serta sampai perhitungan pengukuran parameters bandwidth, delay dan packet loss.

### Skenario Simulasi Serangan

Pada bagian ini akan dijelaskan melakukan serangan dan melakukan simulasi hingga peneliti mendapatkan data yang di butuhkan untuk Investigasi. Skenario serangan akan dibagi menjadi 4 bagian.

#### 1. Skenario Pertama

Skenario pertama ini dilakukan pada server dengan 1 attacker melakukan serangan sebesar 30.000, 50.000, dan 100.000 paket sebanyak 20 kali. Percobaan ini dilakukan untuk mengetahui waktu yang dibutuhkan server untuk menerima paket.

#### 2. Skenario Kedua

Skenario pertama ini dilakukan pada 1 attacker melakukan serangan sebesar 30.000, 50.000, dan 100.000 paket sebanyak 20 kali. Pada skenario kedua ini dilakukan pengamatan terhadap kinerja server dan dilakukan untuk mengambil traffic jaringan terhadap serangan dan pengukuran kinerja *Quality of Service (QoS)*.

3. Skenario Ketiga

Skenario pertama ini dilakukan pada server dengan 2 attacker melakukan serangan sebesar 30.000, 50.000, dan 100.000 paket sebanyak 20 kali. Percobaan ini dilakukan untuk mengetahui waktu yang dibutuhkan server untuk menerima paket.

4. Skenario Keempat

Skenario pertama ini dilakukan pada server dengan 2 attacker melakukan serangan sebesar 30.000, 50.000, dan 100.000 paket sebanyak 20 kali. Pada skenario kedua ini dilakukan pengamatan terhadap kinerja server dan dilakukan untuk mengambil traffic jaringan terhadap serangan dan pengukuran kinerja *Quality of Service (QoS)*.

3. Hasil dan Pembahasan

Data skenario pertama yaitu serangan yang ditujukan kepada server dengan 1 attacker dengan besar paket yang di kirim 30.000 paket, 50.000 paket dan 100.000. paket setelah dilakukan penyerangan berikut data yang di dapat seperti pada tabel 4.1.

Table 1 Hasil Data Skenario Pertama

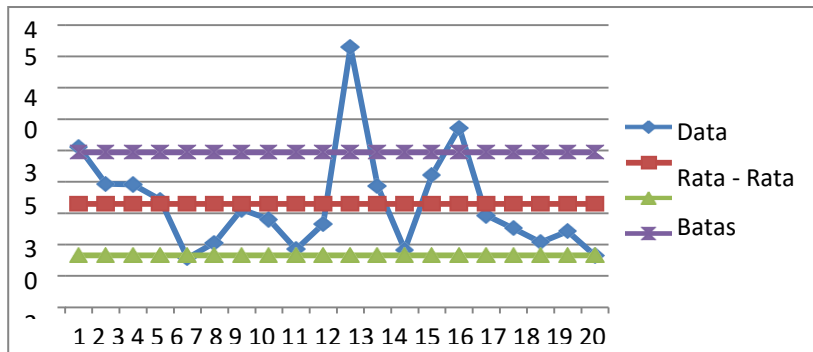
No	ATTACK 1 PC		
	30.000 Paket	50.000 Paket	100.000 Paket
1	25.57	16.42	20.98
2	19.69	22.33	14.73
3	19.57	12.72	26.17
4	17.16	13.98	13.06
5	7.84	19.12	8.69
6	10.29	7.91	10.95
7	15.57	13.71	9.85
8	14.01	8.96	9.47
9	9.22	12.8	8.33
10	13.25	10.33	36.39
11	41.48	13.75	11.42
12	19.28	9.79	9.18
13	9.17	9.33	12.04
14	21.08	18.74	9.9
15	28.63	10.26	8.98
16	14.65	11.01	11.04
17	12.56	32.16	11.5
18	10.35	11.57	9.84
19	12.12	13.61	20.83
20	8.24	26.03	16.34

Dari hasil table 1 skenario pertama memiliki satuan detik, setiap percobaan yang dilakukan menghasilkan data yang berbeda, data-data tersebut bisa di lihat di tabel diatas.

Standar Deviasi 30.000 Paket Pada Attack 1 PC

- 1 Rata – rata ( $\bar{x}$ ) = 16.49 detik.
- 2 Data Dikurangi Rata-rata = data di kurangi hasil rata -rata 3.  
Variansi = 1277.3753 / 19 = 67.23027895

4. Standar Deviasi =  $67.23027895^{-2} = 8.199407231$
5. Menentukan Batas Bawah dan Batas Atas
  - a. Batas Bawah =  $16.49 - 8.199407231 = 8.290592769$
  - b. Batas Atas =  $16.49 + 8.199407231 = 24.68940723$

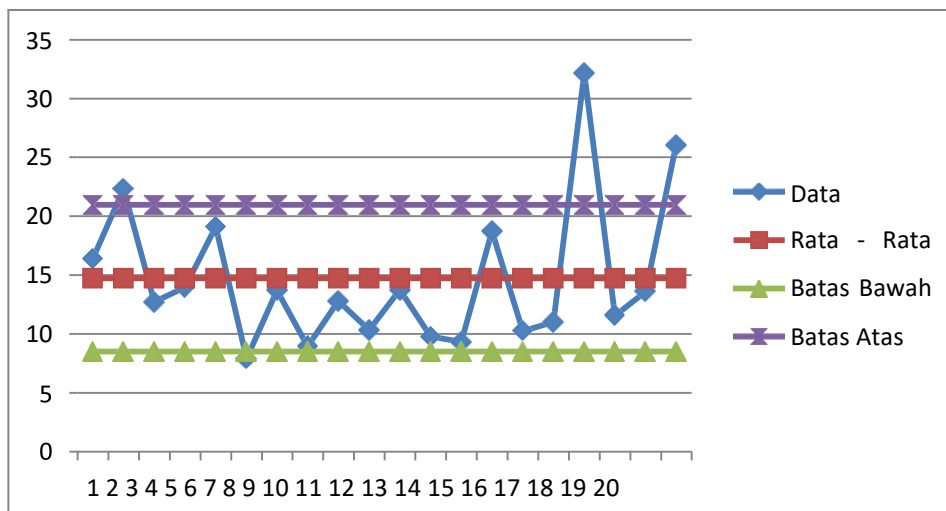


Gambar 3 Attack 1 PC 30.000 Paket

Pada grafik yang terdapat pada gambar 3 didapatkan dua data yang menunjukkan melebihi dari batas atas, dan kebanyakan data menunjukkan di bawah dari rata rata.

Standar Deviasi 50.000 Paket Pada Attack 1 PC

- 1 Rata – rata ( $\bar{x}$ ) = 14.73 detik.  
 Rata – rata ( $\bar{x}$ )
- 2 Data Dikurangi Rata-rata = data di kurangi hasil rata -rata 3.  
 Variansi =  $735.5797 / 19 = 38.71472105$
4. Standar Deviasi =  $38.71472105^{-2} = 6.22211548$
5. Menentukan Batas Bawah dan Batas Atas
  - a. Batas Bawah =  $14.73 - 6.22211548 = 8.50788452$
  - b. Batas Atas =  $14.73 + 6.22211548 = 20.95211548$



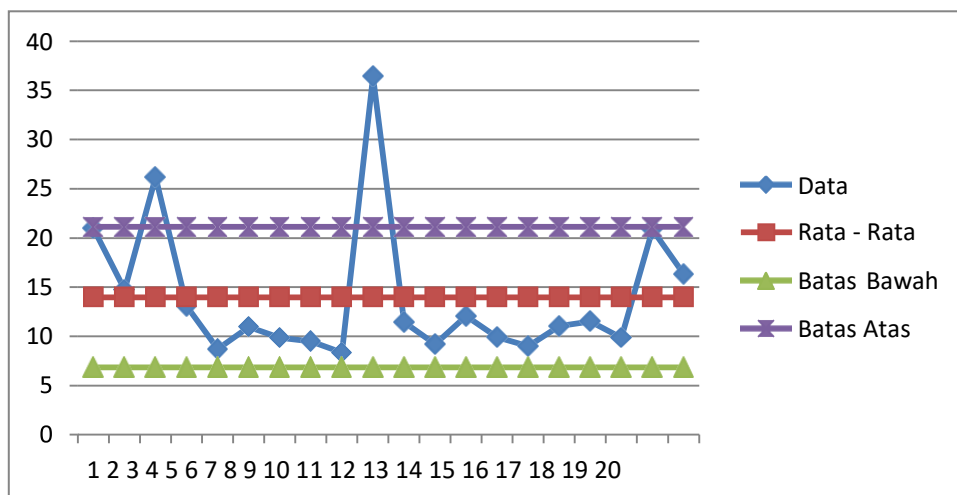


Gambar 4 Attack 1 PC 50.000 Paket\

Pada grafik yang terdapat pada gambar 4. didapatkan empat data yang menunjukkan melebihi dari batas atas, dan kebanyakan data menunjukkan dibawah dari batas rata - rata.

Standar Deviasi 100.000 Paket Pada Attack 1 PC

- 1 Rata – rata ( $\bar{x}$ ) = 13.98 detik.
- 2 Data Dikurangi Rata-rata
3. Variansi =  $967.1269 / 19 = 50.90141579$
4. Standar Deviasi =  $50.90141579^{-2} = 7.134522814$
5. Menentukan Batas Bawah dan Batas Atas
  - a. Batas Bawah =  $13.98 - 7.134522814 = 6.845477186$
  - b. Batas Atas =  $13.98 + 7.134522814 = 21.11452281$



Gambar 5 Attack 1 PC 100.000 Paket

Pada grafik yang terdapat pada gambar 5 didapatkan dua data yang menunjukkan melebihi dari batas atas, dan rata data menunjukkan diatas dari batas bawah.

Hasil Data dan Perhitungan Skenario Ketiga

Data skenario ketiga yaitu serangan yang ditujukan kepada server dengan 2 attacker besar paket yang di kirim 30.000 paket, 50.000 paket dan 100.000 paket setelah dilakukan penyerangan berikut data yang di dapat seperti pada tabel 2

Table 2 Hasil Data Paket Skenario Ketiga

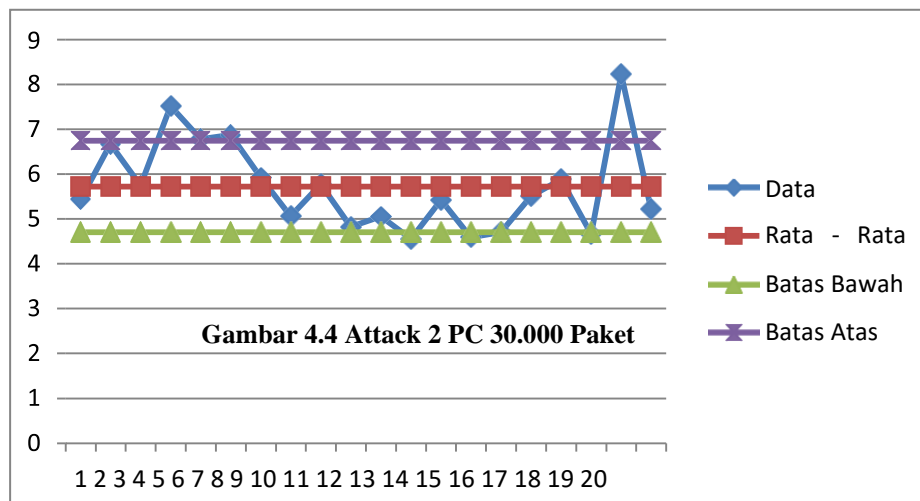
No	ATTACK 2 PC		
	30.000 Paket	50.000 Paket	100.000 Paket
1	5.43	4.06	4.4
2	6.67	5.92	4.64
3	5.74	7.03	7.26

4	7.51	6.53	4.96
5	6.78	5.29	5.38
6	6.87	5.26	5.09
7	5.92	5.93	8.37
8	5.06	5.61	8.16
9	5.77	9.2	6.23
10	4.82	7.89	5.45
11	5.05	5.01	5.57
12	4.55	4.4	6.08
13	5.42	6.19	4.78
14	4.59	5.43	5.19
15	4.7	6.17	6.11
16	5.51	7.9	5.28
17	5.88	6.86	4.81
18	4.66	4.72	5.97
19	8.22	4.74	4.64
20	5.21	4	5.82

Standard deviasi yang dihitung untuk menentukan klasifikasi serangan dinilai cepat atau lambat.

#### Standar Deviasi 30.000 Paket Pada Attack 2 PC

- 1 Rata – rata ( $\bar{x}$ ) = 5.72 detik
- 2 Data Dikurangi Rata-rata
3. Variansi =  $19.8538 / 19 = 1.0449368$
4. Standar Deviasi =  $1.0449368^{-2} = 1.022221523$
5. Menentukan Batas Bawah dan Batas Atas
  - a. Batas Bawah =  $5.72 - 1.022221523 = 4.697778477$
  - b. Batas Atas =  $5.72 + 1.022221523 = 6.742221523$

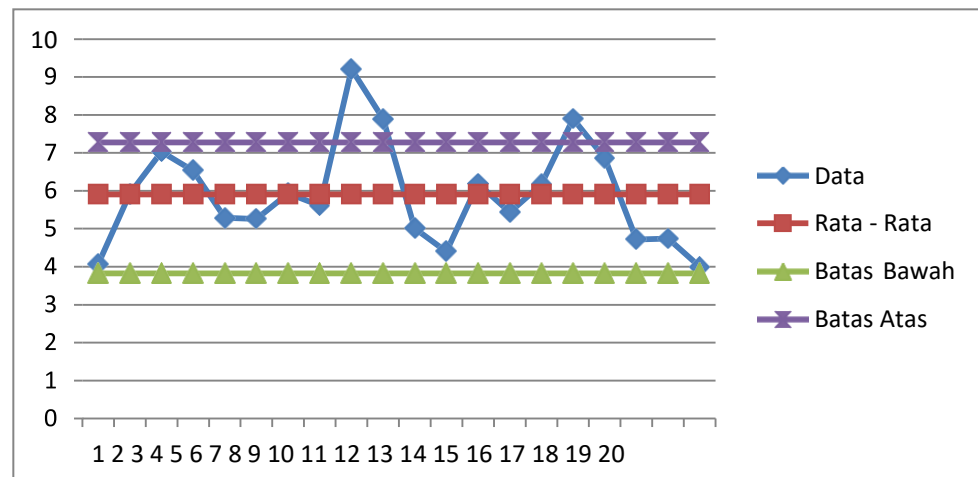


Gambar 6 Attack 2 PC 30.000 Paket

Pada grafik yang terdapat pada gambar 6 didapatkan dua data yang menunjukkan melebihi dari batas atas, dan rata rata data menunjukkan diatas dari batas bawah.

Standar Deviasi 50.000 Paket Pada Attack 2 PC

- 1 Rata – rata ( $\tilde{\phantom{x}}$ ) = 5.91 detik
- 2 Data Dikurangi Rata-rata
3. Variansi =  $35.4654 / 19 = 1.8666$
4. Standar Deviasi =  $1.8666^{-2} = 1.366235704$
5. Menentukan Batas Bawah dan Batas Atas
  - a. Batas Bawah =  $5.91 - 1.366235704 = 3.823764296$
  - b. Batas Atas =  $5.91 + 1.366235704 = 7.276235704$



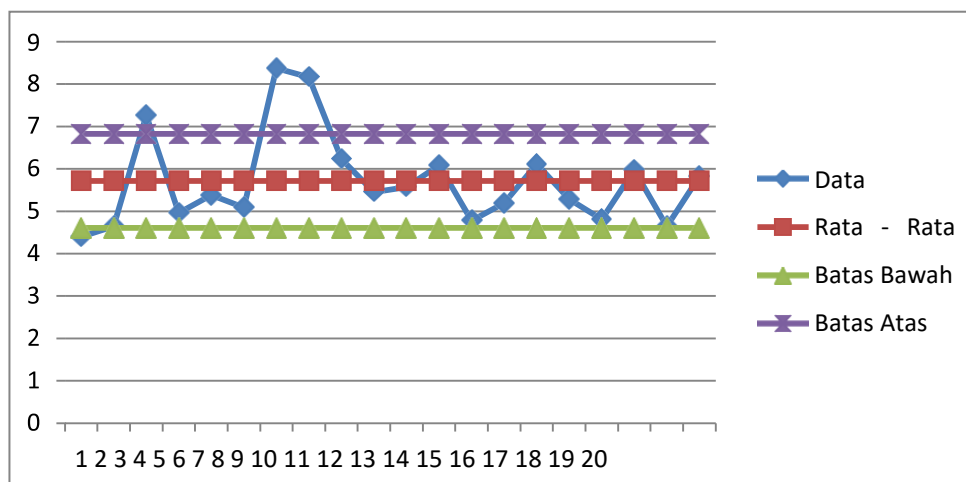
Gambar 7 Attack 2 PC 50.000 Paket

Pada grafik yang terdapat pada gambar 7 didapatkan dua data yang menunjukkan melebihi dari batas atas, dan rata rata data menunjukkan diatas dari batas bawah.

Standar Deviasi 100.000 Paket Pada Attack 2 PC

- 1 Rata – rata ( $\tilde{\phantom{x}}$ ) = 5.71 detik
- 2 Data Dikurangi Rata-rata
3. Variansi =  $23.4067 / 19 = 1.231931579$
4. Standar Deviasi =  $1.231931579 = 1.109924132$
5. Menentukan Batas Bawah dan Batas Atas

- a. Batas Bawah =  $5.71 - 1.109924132 = 4.600075868$
- b. Batas Atas



Gambar 8 Attack 2 PC 100.000 Paket

Pada grafik yang terdapat pada gambar 8 didapatkan tiga data yang menunjukkan melebihi dari batas atas, dan rata data menunjukkan diatas dari batas bawah.

#### 4.Kesimpulan

Hasil pengujian serangan Distributed Denial of Service : jika serangan tidak banyak looping atau perulangan maka akan berpengaruh kepada memori dan jika seran serangan banyak menggunakan looping atau perulangan akan berpengaruh kepada prosessor.

#### DAFTAR PUSTAKA

Faizin, R. N. (2014). Implementasi Machine Learning Sebagai Kontrol Quality of Service (QoS) Pada Jaringan Komputer. Yogyakarta: UIN Sunan Kalijaga.

Ferdiansyah, P. D. (2013). Analisis Quality of Service Private Cloud Computing Dengan Pengujian Serangan Denial of Service Pada Platform Eucalyptus.

Hamdan, R. (2013, Mei 15). Tools Jaringan: Net Tools. Dipetik Maret 9, 2017, dari <https://www.rangghamdan.com/2013/05/15/tools-jaringan-net-tools/>: <https://www.rangghamdan.com>

Hasibuan, Z. (2007). Metodologi Penelitian Pada Bidang Ilmu Komputer dan Teknologi Informasi. Jakarta: Fakultas Ilmu Komputer Universitas Indonesia.

Jusak. (2013). Teknologi Komunikasi Data Modern. Yogyakarta: Andi.

Kamarullah,A.Hafiz. (2009). Penerapan Metod Quality of Service pada jaringan Traffic yang padat. Jurnal jaringan komputer universitas sriwijaya.

Komputer, W. (2003). Konsep Jaringan Komputer dan pengembangannya.

Yogyakarta: Salemba infotek.

Kurniawan, A. (2015, Juni 13). 13 pengertian analisis menurut para ahli didunia.

Diambil kembali dari <http://www.gurupendidikan.com>:

<http://www.gurupendidikan.com/13-pengertian-analisis-menurut-para-ahli-didunia/>

Kusuma, R. A. (2014). *Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO 27001 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta*. Yogyakarta: UIN Sunan Kalijaga.

MADCOMS. (2009). *Membangun Sistem Jaringan Komputer*. Yogyakarta: Andi.

Miftahul Huda, J. (2013). *Analisis Karakteristik Lalu Lintas Data Internet Aplikasi Wew Social Network*.

Nugroho, Y. S. (2015). *Investigasi Forensik Jaringan Dari Serangan DDOS Menggunakan Metode Naive Bayes*. Yogyakarta: UIN Sunan Kalijaga.

Nurmalia. (2010). *Pengukuran Interferensi Pada Access Point(AP) Untuk Mengetahui Quality of Service (QoS)*. Jakarta: UIN Syarif Hidayatullah. Paul, F., & Huston, G. (1998). *Quality of Service: Delivering QoS on the Internet and in Corporate Networks*. New York: NY USA.

Polit; D.F. & Hungler; B.P. (1999). *Nursing Reasearch Principle and Methods*. NY-Baltimore-Philadelphia: Lippincott.

Prabowo, A. M. (2017). *Analisis Keamanan WLAN Terhadap Gangguan ARP Spoofing (Studi Kasus Kantor Dinas Kebudayaan dan Pariwisata Kabupaten Boyolali)*. Yogyakarta: UIN Sunan Kalijaga.

Pratama, I. A. (2014). *Handbook Jaringan Komputer*. Bandung: Informatika Bandung.

Priyambodo, T. K., & heriadi, d. (2005). *Jaringan Wi-Fi, Teori & Implementasi*. Yogyakarta: Andi.

Rifai, A. A. (2011). *Analisa dan Implementasi Quality of service (Qos) pada Router OS Mikrotik*. Yogyakarta: UIN Sunan Kalijaga.

Romadhon, P. P. (2014). *Analisis Kinerja Jaringan Wireless Lan Menggunakan Metode Qos Dan Rma Pada PT Pertamina Ep Ubep Ramba (Persero)*. Palembang: Universitas Bina Darma.

Romadhona, F. Y. (2012). *Optimalisasi Jaringan Wireles dengan QoS Berbasis Algoritma Hierarchical Token Bucket (HTB)*. Yogyakarta: UIN Sunan Kalijaga..