DETEKSI SERANGAN DDOS UDP FLOOD DENGAN METODE RULE-BASED SIGNATURE SECARA REAL-TIME DI JARINGAN SDN

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

EPRIYADI
09011281419046

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019

LEMBAR PENGESAHAN

DETEKSI SERANGAN DDOS UDP FLOOD DENGAN METODE RULE-BASED SIGNATURE SECARA REAL-TIME DI JARINGAN SDN

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

EPRIYADI
09011281419046

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, S.T., M.Eng.
NIP 197806112010121004

Indralaya, Juli 2019
Pembimbing ,

Deris Stiawan, M.T., Ph.D.
NIP 197806172006041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 02 Juli 2019

Tim Penguji :

1. **Ketua** : **Ahmad Heryanto, S.Kom., M.T.** (.....)
2. **Anggota I** : **Huda Ubaya, M.T.** (.....)
3. **Anggota II** : **Firdaus, M.Kom.** (.....)

Mengetahui,
Ketua Jurusan Sistem Komputer

Rossi Passarella, M. Eng.
NIP. 19780611 201012 1 004

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Epriyadi

NIM : 09011281419046

Program Studi : Sistem Komputer

Judul : Deteksi Serangan DDoS Udp Flood Dengan Metode Rule-Based Signature Secara Real-Time Di Jaringan SDN

Hasil Pengecekan *Software iThenticate/Turnitin* : 18%

Menyatakan bahwa laporan Tugas Akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/*plagiat.* Apabila ditemukan unsur penjiplakan /*plagiat* dalam laporan Tugas Akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan dalam keadaan sadar dan tidak dipaksakan.

Indralaya, Juli 2019

Epriyadi

NIM. 09011281419046

HALAMAN PERSEMBAHAN

Motto :

" Tak Ada Gunung Setinggi Tekadku, Tak Ada Sungai Sederas Semangatku"

Dengan Mengucap Syukur Allhamdulilah atas rahmat dari allah SWT, aku persembahkan karya kecil ini untuk :

- Emak dan Bak Tercinta
- Saudaraku Yandi Anggara, Ayu Puspita Safitri dan Rayhan Hidayat
- Seluruh Keluarga Besar
- Teman-Teman SK 2014 Seperjuangan
- Almamaterku

KATA PENGANTAR

Puji dan syukur penulis persembahkan kepada Allah SWT atas segala rahmat yang telah diberikan, sehinngga penulis dapat menyelesaikan laporan Tugas Akhir dengan judul "**Deteksi Serangan DDoS Udp Flood Dengan Metode Rule-Based Signature Secara Real-Time Di Jaringan SDN**".

Shalawat serta salam tidak lupa penulis ucapkan kepada baginda Rasullulah Muhammad SAW yang telah menjadi teladan bagi umat manusia sehingga kehidupan manusia sekarang bias lebih baik terutama dalam bidang ilmu pengetahuan.

Dalam penulisan tugas akhir ini penulis menyadari bahwa penulis banyak mendapatkan dukungan dari berbagai pihak. Pada kesempatan ini penulis ingin menyampaikan rasa terimakasih kepada semua pihak yang telah meluangkan waktu, tenaga dan pikirannya dalam membantu penulis sehingga penulis bisa menyelesaikan skripsi ini. Rasa terimakasih penulis ucapkan kepada:

1. Keluarga terinta, Mak, Bak, Kakak, dan kedua Adikku yang selalu memberikan dukungan doa sehingga pada akhirnya tugas ini dapat diselesaikan dengan perasaan bangga dan puas.
2. Bapak Deris Stiawan, M.T., Ph.D selaku Pembimbing Tugas Akhir sekaligus Pembimbing Akademik yang telah memberi bimbingan dan dukungan dalam penyelesaian penulisan tugas akhir. Terima Kasih sebesar-besarnya saya ucapkan kepada beliau.
3. Bapak Huda Ubaya, M.T., dan Bapak Firdaus, M.Kom. selaku dosen penguji sidang Tugas Akhir yang telah memberi banyak masukan berupa kritik dan saran sehingga konten dari laporan ini menjadi lebih baik.
4. Bapak Rossi Passarella, M.Eng selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.

5. Bapak, Ibu Dosen Jurusan Sistem Komputer yang selama ini telah memberikan dan menyalurkan ilmu dan pengalamannya.
6. Keluarga Besar LPM Gelora Sriwijaya, Para Senior 01 sampai 15 serta terkhusus seangkatan *"16". " Salam Pers Mahasiswa!!".*
7. Keluarga Besar Himpala Bhuwana Cakti, Para Senior ALB dari PRS sampai RGL dimanapun berada terima kasih yang sebesar besarnya. Terkhusus satu bivak Alam Lintas Sumatera. "*Salam Lestari !*".
8. Semua teman-teman angkatan 2014 yang sama-sama menjalankan suka duka perkuliahan, terkhusus HSH member(Aidil, Anggit, Fahron, Ridwan, Sigit, Randa, Yonathan, Uda, Dayat), mastah koding yang melegenda Faris.
9. Kakak dan adik tingkat SK, yang tidak bisa saya sebutkan satu persatu.
10. Keluarga Besar Kak Andi yang telah mensupport saat awal perkuliahan.
11. Luluk Mastiti yang telah menemani saat pengerjaan tugas akhir dan memberikan motivasi serta semangat dan doa kepada penulis.

Semoga dengan terselesainya tugas akhir ini dapat bermanfaat untuk menambah wawasan dan pengetahuan bagi kita semua. Dalam penulisan laporan ini penulis menyadari bahwa masih ada banyak kekurangan dan ketidaksempurnaan, oleh karena itu penulis mohon kritik dan saran yang membangun untuk Perbaikan Laporan Tugas Akhir ini, agar menjadi lebih baik dimasa yang akan datang.

Indralaya, Juli 2019

Penulis

DETEKSI SERANGAN DDOS UDP FLOOD DENGAN METODE RULE-BASED SIGNATURE SECARA REAL-TIME DI JARINGAN SDN

Epriyadi (09011281419046)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : epriyadi@outlook.com

Abstrak

Penelitian ini berfokus pada serangan DDoS UDP Flood dimana lalu lintas data dikategorikan sebagai data normal atau *anomaly*. Paket yang dikirim merupakan paket UDP melalui jaringan SDN dalam virtualisasi mininet dengan menggunakan *POX Controller*. Ekstraksi data dilakukan untuk menentukan atribut unik yang akan digunakan pada algoritma *Rule-Based* untuk mendeteksi serangan DDoS UDP Flood dalam lingkungan *real-time*. Hasil yang didapat pada penelitian ini berupa pengelompokan data normal dan data serangan kemudian akurasi dari pengelompokan tersebut akan dihitung menggunakan *confusion matrix*. System IDS yang dibangun menggunakan metode *rule-base* lebih baik dalam mendeteksi serangan DDoS UDP Flood dibuktikan dengan akurasi mencapai 98,4% dibandingkan dengan Snort IDS yang hanya 94%.

Kata Kunci: *Rule-Based, DDoS, Mininet, SDN, IDS, Confusion Matrix*

UDP FLOOD DDOS ATTACK DETECTION BY THE METHOD OF RULE-BASED SIGNATURES IN REAL-TIME ON NETWORK SDN

Epriyadi (09011281419046)

Department Of Computer Engineering, Faculty Of Computer Science,

Sriwijaya University

Email : epriyadi@outlook.com

Abstract

This research focuses on the UDP Flood DDoS attacks where traffic data is categorized as normal data or anomaly. Packages are sent via UDP packet network is SDN in mininet virtualization using POX Controller. Data extraction was performed to determine the unique attribute that will be used on a Rule-Based algorithm to detect a UDP Flood DDoS attack in a real-time environment. The results obtained in this research in the form of a normal data clustering and data attacks then the accuracy of the grouping will be calculated using the confusion matrix. System IDS that are built using the method of rule-base better in detecting UDP Flood DDoS attack attested with accuracy reaching 98.4% compared with Snort IDS that only 94%.

Keyword: *Rule-Based, DDoS, Mininet, SDN, IDS, Confusion Matrix*

DAFTAR ISI

Halaman

HALAMAN JUDUL i
HALAMAN PENGESAHAN ii
HALAMAN PERSETUJUAN iii
HALAMAN PERNYATAAN iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
ABSTRAK ix
ABSTRACT x
DAFTAR ISI xi
DAFTAR GAMBAR xiv
DAFTAR TABEL xvi

BAB I. PENDAHULUAN

1.1 Latar Belakang 1
1.2 Tujuan 2
1.3 Manfaat 3
1.4 Perumusan Masalah 3
1.5 Batasan Masalah 3
1.6 Metodologi Penelitian 4
1.7 Sistem Penelitian 5

BAB II. TINJAUAN PUSTAKA

2.1 Distributed Denial of Service 6
2.2 UDP 8
2.3 UDP Flood 9

2.4	Data Mining	9
2.5	Signature-Based Detection IDS	9
2.6	Anomaly-Based Detection IDS	10
2.7	Hybrid-Based Detection IDS	10
2.8	Intrusion Detection System	11
2.8.1	Jenis-Jenis Intrusion Detection System	11
2.9	Snort Intrusion Detection System	12
2.9.1	Sniffer Mode	12
2.9.2	Intrusion detection Mode	13
2.9.3	Komponen Komponen Snort IDS	13
2.9.4	Prioritas Snort Rules	14
2.10	Real-Time	16
2.10.1	Jenis-Jenis Real-Time	16
2.10.2	Karakteristik Sistem Real-Time	16
2.11	DVWA	17
2.12	Data Exstraction	17
2.13	Confusion matrix	17
2.14	Software Defined Network	19
2.15	Jaringan traditional vs Jaringan SDN Openflow	20
2.16	Openflow	21

BAB III. METODOLOGI

3.1	Pendahuluan	23
3.2	Kerangka Kerja Penelitian	23
3.3	Perancangan System	25
3.3.1	Perancangan Topologi	25
3.3.2	Kebutuhan Perangkat Keras (*Hardware*)	26
3.3.3	Kebutuhan Perangkat Lunak (*Software*)	26
3.4	Snort Sebagai NIDS	26
3.4.1	*Engine IDS*	27

3.5 Skema Sistem Pembelajaran 28
3.6 Program Deteksi Support Vector Machine 29
3.6.1 Flowchart Support Vector Machine 30
3.7 Mengenali Pola Serangan DDoS UDP Flood 31
3.8 Skenario Pengujian 32
3.10 Hasil dan Analisis 33

BAB IV. HASIL DAN PEMBAHASAN SEMENTARA

4.1 Pendahuluan 34
4.2 DDoS UDP Flood 34
4.3 Analisa Dataset 36
4.4 Perbedaan Paket Normal Dan Serangan 37
4.5 Hasil Feature Extraction 38
4.6 Validasi Hasil Feature Extraction 39
4.7 Pengenalan Pola Serangan DDoS UDP Flood 40
4.8 Pengujian IDS Dataset 41
4.9 Pengujian System Deteksi Real-Time menggunkan Metode Rule-Base 43
4.10 Hasil Pengolahan Data 46

BAB V. KESIMPULAN

5.1 Kesimpulan 49
5.2 Saran 50

DAFTAR PUSTAKA

LAMPIRAN-LAMPIRAN

DAFTAR ISI

Halaman

HALAMAN JUDUL i
HALAMAN PENGESAHAN ii
HALAMAN PERSETUJUAN iii
HALAMAN PERNYATAAN iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
ABSTRAK viii
ABSTRACT ix
DAFTAR ISI x
DAFTAR GAMBAR xiii
DAFTAR TABEL xv

BAB I. PENDAHULUAN

1.1 Latar Belakang 1
1.2 Tujuan 2
1.3 Manfaat 3
1.4 Perumusan Masalah 3
1.5 Batasan Masalah 3
1.6 Metodologi Penelitian 4
1.7 Sistem Penelitian 5

BAB II. TINJAUAN PUSTAKA

2.1 Distributed Denial of Service 6
2.2 UDP 8
2.3 UDP Flood 9

2.4	Data Mining	9
2.5	Signature-Based Detection IDS	9
2.6	Anomaly-Based Detection IDS	10
2.7	Hybrid-Based Detection IDS	10
2.8	Intrusion Detection System	11
2.8.1	Jenis-Jenis Intrusion Detection System	11
2.9	Snort Intrusion Detection System	12
2.9.1	Sniffer Mode	12
2.9.2	Intrusion detection Mode	13
2.9.3	Komponen Komponen Snort IDS	13
2.9.4	Prioritas Snort Rules	14
2.10	Real-Time	16
2.10.1	Jenis-Jenis Real-Time	16
2.10.2	Karakteristik Sistem Real-Time	16
2.11	DVWA	17
2.12	Data Exstraction	17
2.13	Confusion matrix	17
2.14	Software Defined Network	19
2.15	Jaringan traditional vs Jaringan SDN Openflow	20
2.16	Openflow	21

BAB III. METODOLOGI

3.1	Pendahuluan	23
3.2	Kerangka Kerja Penelitian	23
3.3	Perancangan System	25
3.3.1	Perancangan Topologi	25
3.3.2	Kebutuhan Perangkat Keras (*Hardware*)	26
3.3.3	Kebutuhan Perangkat Lunak (*Software*)	26
3.4	Snort Sebagai NIDS	26
3.4.1	*Engine IDS*	27

3.5	Skema Sistem Pembelajaran	28
3.6	Program Deteksi Support Vector Machine	29
3.6.1	Flowchart Support Vector Machine	30
3.7	Mengenali Pola Serangan DDoS UDP Flood	31
3.8	Skenario Pengujian	32
3.10	Hasil dan Analisis	33

BAB IV. HASIL DAN PEMBAHASAN SEMENTARA

4.1	Pendahuluan	34
4.2	DDoS UDP Flood	34
4.3	Analisa Dataset	36
4.4	Perbedaan Paket Normal Dan Serangan	37
4.5	Hasil Feature Extraction	38
4.6	Validasi Hasil Feature Extraction	39
4.7	Pengenalan Pola Serangan DDoS UDP Flood	40
4.8	Pengujian IDS Dataset	41
4.9	Pengujian System Deteksi Real-Time menggunkan Metode Rule-Base	43
4.10	Hasil Pengolahan Data	46

BAB V. KESIMPULAN

5.1	Kesimpulan	49
5.2	Saran	50

DAFTAR PUSTAKA

LAMPIRAN-LAMPIRAN

DAFTAR GAMBAR

		Halaman
Gambar 2.1	Mekanisme serangan DDoS	7
Gambar 2.2	UDP header	8
Gambar 2.3	Komponen *Snort IDS*	14
Gambar 2.4	Arsitektur jaringan tradisional dan SDN	20
Gambar 2.5	Spesifikasi Switch Openflow	21
Gambar 3.1	Kerangka kerja penelitian	24
Gambar 3.2	Topologi Dataset	25
Gambar 3.3	Struktur Snort Rules	27
Gambar 3.4	Format *Rules Snort*	27
Gambar 3.5	Skema pembelajaran visualisasi	28
Gambar 3.6	Skema deteksi real-time	29
Gambar 3.7	Rules DDoS UDP Snort	29
Gambar 3.8	Pola serangan DDoS UDP Flood terdeteksi snort	30
Gambar 3.9	Skema Pengambilan Dataset	31
Gambar 3.10	Flowchart Rule-Based Signature	32
Gambar 4.1	Sambungan dari bot ke master	34
Gambar 4.2	Melakukan serangan DDoS UDP Flood	35
Gambar 4.3	Tapping data dari Controller Pox	36
Gambar 4.4	Hasil ekstraksi dan raw data paket normal.pcap	38
Gambar 4.5	Hasil ekstraksi dan raw data paket serangan.pcap	39
Gambar 4.6	Korelasi antara feature ekstraction dan raw data pcap	39
Gambar 4.7	Korelasi antara feature ekstraction dan Snort	40

Gambar 4.8 Korelasi alert snort, rules snort dan feature ekstraction 42

Gambar 4.9 Melakukan serangan DDoS UDP Flood 44

Gambar 4.10 Hasil Deteksi Real-time menggunakan Rule-Based 44

Gambar 4.11 Validasi antara raw data(.pcap) dengan alert engine IDS 45

Gambar 4.12 Perbandingan Binnary Clasification 47

Gambar 4.13 Perbandingan Detection Rate 48

DAFTAR TABEL

		Halaman
Tabel 2.1	Tingkat prioritas pada *rules snort*	14
Tabel 2.2	Tipe Alert pada confussion matrix	18
Tabel 3.1	Spesifikasi kebutuhan perangkat lunak	26
Tabel 3.2	*Action rules snort*	28
Tabel 3.3	Skema pengambilan dataset	31
Tabel 4.1	Data pcap yang akan dianalisa	36
Tabel 4.2	Jumlah traffic data	37
Tabel 4.3	Perbedaan paket normal dan serangan	38
Tabel 4.4	Atribut pola serangan DDoS UDP Flood	41
Tabel 4.5	Hasil pengujian	41
Tabel 4.6	*Confussion Matrix*	46
Tabel 4.7	Nilai detection rate confussion matrix	47

BAB I. PENDAHULUAN

1.1 Latar Belakang

Pada penelitian [1] tentang Visualisasi Serangan *Remote to Local* (R2L) Dengan *Clustering K-Means*. Hasilnya Pola serangan R2L pada dataset DARPA dapat dikenali dengan beberapa paramer seperti *source address, destination address, flags, ip length,* dan *tcp length.*

Visualisasi dapat membantu user untuk mendeteksi pola serangan dengan lebih cepat, dan apabila dikombinasikan dengan teknologi seperti *data mining* atau *machine learning*, sistem visualisasi akan lebih efektif dalam mendeteksi pola serangan[1].

Beberapa penelitian menyarankan untuk menerapkan teknik visualisasi kelingkungan *real-time* [1] [2]. Dengan memvisulisasikan serangan, akan lebih mudah dalam mengenali dan menyimpulkan pola dari gambar visual yang komplek [2].

Telah banyak penelitian yang dilakukan untuk mencari metode terbaik dalam memvisualisasikan serangan. Diantaranya penelitian [4], membahas permasalahan terhadap visualisasi serangan secara otomatis menggunakan *parallel coordinate attack visualization* (PCAV).

Penelitian [3] mendeteksi serangan internet dalam skala besar yang tidak diketahui seperti *internet worms, DoS attack* dan aktifitas *network scanning*. PCAV menampilkan *traffic* jaringan pada bidang koordinat paralel menggunakan informasi seperti *source IP address, destination IP address, source port* dan *packet length.*

Pengujian secara *real-time* membuktikan bahwa penerapan fungsi *complete/incomplete connection record* dalam proses *preprocessing* pembentukan data audit atau *connection record* dapat menjadi solusi permasalahan keterlambatan pendeteksian akibat durasi koneksi yang terlalu lama [5]. Masih banyak jenis serangan terhadap jaringan yang perlu diteliti untuk divisualisasikan diantarannya serangan *Distributed Denial of Services*(DDoS).

DDoS merupakan jenis serangan dengan volume, intensitas, dan biaya mitigasi yang terus meningkat seiring berkembangnya skala organisasi[6]. Dalam kasus serangan DDoS beberapa penelitian mengenai pendeteksian telah dilakukan.

Diantaranya penelitian [7] menganalisis nilai entropi artefak jaringan dalam kondisi jaringan normal dan abnormal yang dipengaruhi oleh DoS, *port scanning* dan *worm* menghasilkan kesimpulan bahwa nilai entropi dari artefak jaringan saling berkorelasi. Memanfaatkan fungsi entropi maksimal untuk membangun angka distribusi jaringan yang normal dan kemudian menggunakan entropi relatif untuk mendeteksi anomali/serangan DDoS.

Pada penelitian [8] menggunakan model distribusi jaringan yang didasarkan pada atribut TCP/IP sehingga menghasilkan kombinasi atribut yang cukup besar. Paket data artefak jaringan harus diberi label dan diurutkan sehingga langkah *preprocessing* menjadi kompleks dan menurunkan kemampuan untuk mendeteksi serangan DDoS secara cepat.

Metode lainnya yang dianggap telah berhasil dalam melakukan pendeteksian terhadap serangan yaitu *Support Vector Machine* (SVM). Dengan merujuk pada penelitian [9] tentang menganalisis perbandingan metode yang dihasilkan dari proses klasifikasi serangan DoS berdasarkan nilai akurasi *confusion matrix, precision, recall, dan f1 score. Naive Bayes, SVM Linear, SVM Polynomial* dan *SVM Sigmoid* menghasilkan persentase akurasi berturut-turut sebesar 85,055%, 99,995%, 99,999%, dan 99,995%. Persentase akurasi tertinggi diperoleh SVM *Polynomial, sedangkan Naive Bayes* menghasilkan persentase akurasi terendah.

Berdasarkan uraian diatas penelitian ini bertujuan untuk mengembangkan sebuah pendekatan baru untuk mendeteksi dan memvisualisasikan serangan DDoS secara *Real-Time*, yaitu menggunakan metode *Rule Base*.

1.2 Tujuan

Adapun tujuan dari penelitian ini yaitu :

1. Mengenali pola serangan *DDoS UDP Flood* pada jaringan SDN.
2. Membuat algoritma yang mampu mendeteksi pola serangan *DDoS UDP Flood* .

3. Menerapkan metode *Rule Base* untuk mengklasifikasikan trafik data serangan maupun Normal.
4. Membuat algoritma untuk memvisualisasikan *DDoS UDP Flood* dalam bentuk grafik.

1.3 Manfaat

Adapun manfaat yang dapat diambil dari penelitian ini adalah:

1. Dapat mendeteksi Serangan *DDoS UDP Flood* secara *real-time* dalam jaringan SDN.
2. Dapat memberikan kemudahan dalam mengetahui pola serangan *DDoS UDP Flood* dalam jaringan SDN.
3. Dapat membedakan pola trafik serangan *DDoS UDP Flood* maupun trafik normal dalam jaringan SDN.

1.4 Perumusan Masalah

Berikut ini merupakan perumusan masalah dalam penelitian ini :

1. Bagaimana mendeteksi serangan *DDoS UDP Flood* secara *real-time* dalam jaringan SDN?
2. Bagaimana mengelompokan trafik serangan maupun trafik normal pada serangan DDoS UDP Flood menggunakan metode *Rule Base*?
3. Bagaimana memvisualisasikan pola serangan *DDoS UDP Flood* kedalam bentuk grafis?

1.5 Batasan Masalah

Agar penelitian mengarah pada pemaparan yang diharapkan, maka diperlukan Batasan masalah dalam penelitian. Adapun Batasan masalah dalam penelitian ini, adalah :

1. Data serangan pada penelitian berfokus pada *DDoS UDP Flood* dalam layanan simulasi *SDN* mengunakan *Mininet.*
2. Data akan dikelompokan menjadi dua bagian, yaitu trafik serangan dan trafik normal.
3. Metode yang digunakan untuk mengelompokan data menggunakan metode *Rule Base.*

4. *Visualisasi* serangan *DDoS UDP Flood* tidak diujikan pada lalu lintas jaringan *real-time*.
5. *Tools* yang digunakan untuk *DDoS UDP Flood* adalah *script* Bahasa *python* yang terdiri dari *Master* dan *Bot* yang dimodifikasi sendiri.
6. Tidak membahas bagaimana cara pencegahan serangan tersebut.
7. Tidak diujikan pada trafik jaringan yang terenkripsi.

1.6 Metodologi Penelitian

Dalam tugas akhir ini terdapat beberapa metodologi yang digunakan, antara lain yaitu :

1. Studi Pustaka/Literatur

   Tahap ini dilakukan dengan cara mempelajari dan mengumpulkan informasi mengenai penelitian yang akan dilakukan. *Literature* tersebut diperoleh dari jurnal, buku, internet dan lain-lain agar dapat menunjang metodologi dan pendekatan yang akan diterapkan pada penelitian.
2. Perancangan Sistem

   Tahap ini membahas mengenai proses yang telah dilakukan dalam membangun sistem dengan menggunakan metode atau pendekatan tertentu. Menentukan perangkat keras, perangkat lunak, jenis topologi yang digunakan dan Bahasa pemrograman yang akan dipakai dalam membangun sistem secara keseluruhan. Kemudian mengimplementasikan algoritam yang dibuat untuk mendeteksi serangan dengan metode *Rule Base*.
3. Pengujian

   Pada tahap ini akan dilakukan pengujian berdasarkan dengan metodologi penelitian sehingga didapatkan hasil uji yang sesuai dengan Batasan masalah dan parameter yang telah ditentukan
4. Analisa

   Hasil dari pengujian akan dianalisa sesuai identifikasi permasalahan. Tahapan ini bertujuan untuk mendapatkan data objektif dari Analisa hasil pengolahan data.
5. Kesimpulan dan Saran

Pada tahap ini dilakukan penarikan kesimpulan dari studi pustaka, metodologi, dan Analisa hasil pengujian. Tahapan ini juga terdapat beberapa poin saran dari penulis untuk penelitian selanjutnya.

1.7 Sistematika Penelitian

Pada tugas akhir ini di buat sistematika penelitan agar mempermudah dalam proses penyusunan dan memperjelas isi dari setiap bab sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi tentang Latar Belakang, Tujuan, Manfaat, Rumusan Masalah, Batasan Masalah, Metodologi Penelitian, dan Sistematika Penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi dasar teori dari penelitan tugas akhir tentang *visualisasi. DDoS UDP Flood, Intrusion Detection System (IDS), real-time, Rule Base* dan teori lainnya yang berhubungan dengan penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan secara bertahap dan terperinci tentang langkah-langkah (metodologi) yang digunakan untuk membuat kerangka berfikir dan kerangka kerja (framework) dalam menyelesaikan tugas akhir.

BAB IV PENGUJIAN DAN ANALISA

Bab ini menjelaskan hasil pengujian yang dilakukan serta analisis dari tiap data yang diperoleh dari hasil pengujian berdasarkan parameter yang telah ditentukan sebelumnya.

BAB V KESIMPULAN SEMENTARA

Bab ini berisi kesimpulan tentang apa yang diperoleh oleh penulis serta merupakan jawaban dari tujuan yang ingin dicapai pada bab 1 (pendahuluan), akan tetapi masih bersifat sementara

DAFTAR PUSTAKA

[1] S. Sandra, D.Stiawan, dan A. Heryanto, "Visualisasi Serangan Brute Force Menggunakan Metode K-Means dan Naïve Bayes," Annu. Res. Semin, Vol. 2, No. 1, pp. 315-320, 2016.

[2] Napsiah, Stiawan,D dan A. Heryanto, "Visualisasi Serangan Denial Of Service Dengan Clustering Menggunakan K-Means Algorithm," Annu. Res. Semin, Vol. 2, No. 1, pp. 348-352, 2016.

[3] Y.-J. Yang dan Y.-H. Liu, "A DoS Attack Situation Visualization Method Based on Parallel Coordinates," IEEE 12th Int. Conf. Comput. Inf. Technol., pp. 340–344, 2012.

[4] H. Choi, H. Lee dan H. Kim, "Fast detection and visualization of network attacks on parallel coordinates," Comput. Secur., vol. 28, no. 5, pp. 276–288, 2009.

[5] Jacobus, A dan Winarko, E. "Penerapan Metode Support Vector Machine pada Sistem Deteksi Intrusi secara Real-time. IJCCS, Vol.8, No. 1, pp. 13-24, 2010.

[6] Rui Zhong dan Guangxue Yue, "DDoS Detection System Based on Data Mining," Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10) Jinggangshan, P. R. China, pp. 062-065, 2010.

[7] Nychis, G., Sekar, V dan Anderson, D. G, "An Empirical Evaluation of Entropy-based Anomaly Detection," Proceedings of the 8th ACM SIGCOMM conference on Internet measurement, Vol. 5, No. 1, pp. 151-156, 2014.

[8] Smith, R., Japkowicz, N., Dondo, M., dan Mason, P, "Using unsupervised learning for network alert correlation. Advances in Artificial Intelligence," Lecturer Notes in Computer Science, Vol. 2, No. 1, pp. 308-319, 2012.

[9] Fluorida. M dan Bhawiyuga. A, "Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan