SISTEM PENCEGAHAN SERANGAN *DDOS TCP FLOOD* MENGGUNAKAN ALGORITMA *INGRESS/EGRESS FILTERING*

MOHAMMAD CAHYADI

09011381621065

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

HALAMAN PENGESAHAN

SISTEM PENCEGAHAN SERANGAN *DDOS TCP FLOOD* MENGGUNAKAN ALGORITMA *INGRESS/EGRESS FILTERING*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarja Komputer

Oleh :

MOHAMMAD CAHYADI
09011381621065

Palembang, Juli 2021

Pembimbing I	**Pembimbing II**
Deris Stiawan, M.T., Ph.D.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 197806172006041002	**NIP. 198701222015041002**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Selasa

Tanggal : 6 Juli 2021

Tim Penguji:

1. **Ketua** : **Ahmad Zarkasi, S.T., M.T.**
2. **Sekretaris** : **Iman Saladin B. Azhar, S.Kom., M.MSI.**
3. **Pembimbing 1** : **Deris Stiawan, M.T., Ph.D.**
4. **Pembimbing 2** : **Ahmad Heryanto, S.Kom., M.T.**
5. **Penguji** : **Sarmayanta Sembiring, S.Si., M.T.**

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERNYATAAN

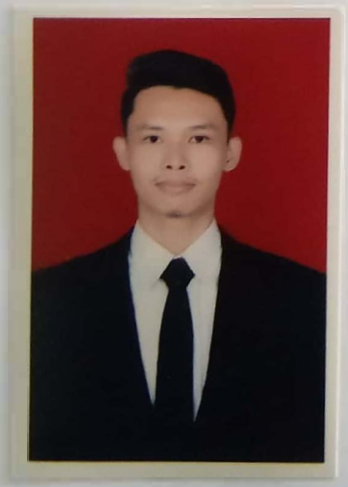
Yang bertanda tangan dibawah ini:

Nama	:	Mohammad Cahyadi
NIM	:	09011381621065
Judul	:	Sistem Pencegahan Serangan *DDoS TCP Flood* Menggunakan Algoritma *Ingress/Egress Filtering*

Hasil pengecekan *Software iThenticate / Turnitin* : 5%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat dari penelitian orang lain. Apabila ditemukan unsur penjiplakan / plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dalam paksaan.



Palembang, Juli 2021
Yang menyatakan,

Mohammad Cahyadi

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Dengan Mengucapkan syukur Alhamdulillah atas Kehadiran Allah SWT dan shalawat serta salam kepada junjungan kita Nabi Muhammad s.a.w, karena atas berkah dan rahmat-Nya jualah penulis dapat menyelesaikan Tugas Akhir ini yang berjudul "**Sistem Pencegahan Serangan *DDoS* TCP Flood Menggunakan Algoritma Ingress/Egress Filtering**", tepat pada waktunya.

Tugas Akhir ini dimaksudkan untuk persyaratan dalam menyelesaikan studi pada jurusan Sistem Komputer Universitas Sriwijaya Palembang. Berdasarkan apa yang penulis dapatkan selama penelitian yang telah dilakukan.

Sebagai manusia yang memiliki kelemahan, penulis menyadari bahwa Tugas Akhir yang dibuat masih jauh dari kata sempurna serta penuh dengan kekurangan, hal ini tidak lain dikarenakan keterbatasan pengetahuan dan pengalaman dari penulis.

Oleh karena itu, penulis sangat mengharapkan adanya masukan-masukan baik berupa kritik maupun saran yang dapat penulis gunakan sebagai bahan perbaikan bagi Tugas Akhir ini. Dalam menyelesaikan Tugas Akhir ini, penulis banyak mendapatkan masukan berupa saran, dorongan, bimbingan serta petunjuk secara langsung dari pembimbing dan banyak pihak lainnya yang sangat membantu terhadap penyelesaian Tugas Akhir ini.

Dengan segala kerendahan hati penulis mengucapkan terima kasih yang sebesar-besarnya dan penghargaan yang sedalam-dalamnya kepada semua pihak yang telah membantu, memberikan petunjuk, dan bimbingan sehingga Tugas Akhir ini dapat diselesaikan dengan baik. Untuk itu, penulis ingin mengucapkan terima kasih kepada :

1. Allah SWT yang telah memberikan berkat dan nikmat kesehatan serta kesempatan kepada penulis sehingga penulis dapat menyelesaikan Tugas Akhir ini.
2. Kedua Orang Tua beserta Kakak yang telah memberikan dukungan baik mental maupun materi sehingga dapat menjalani Pendidikan Strata 1 hingga selesai. Bibi Kasmi dan Mamang Minha, Kak Febri, Kak Heri, Kak Hendra dan Kak Wahyu yang menjadi keluarga kedua diperantauan.
3. Bapak Jaidan Jauhari, S.Pd, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Julian Supardi, M.T. selaku Wakil Dekan Bidang Akademik Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Prof. Dr. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Deris Stiawan, M.T. selaku pembimbing I yang telah banyak memberikan arahan serta motivasi dalam menyelesaikan laporan Tugas Akhir ini
7. Bapak Ahmad Heryanto, S.Kom, M.T. selaku pembimbing II yang telah membimbing dan banyak memberikan arahan kepada penulis dalam menyelesaikan program dan laporan Tugas Akhir ini.
8. Bapak Ahmad Fali Oklilas, M.T. selaku Kepala Laboratorium Elektronika Dasar dan Sistem Digital yang telah memberikan fasilitas dalam melakukan penelitian.
9. M. Nawwar Athalaza, M. Ikshan, Facharudin Abdau, M. Amir Hamzah, Retno Choirunisa, Yogie Alhanif dan Adelia Rizki Putri yang telah mendukung, membantu dan meminjamkan perangkat pribadi mereka untuk kebutuhan selama penelitian.
10. Teman-teman seperjuangan terkhususnya jurusan Sistem Komputer Kampus Palembang Angkatan 2016 yang telah banyak memberikan informasi yang sangat berguna.
11. Semua pihak yang tidak dapat disebutkan satu persatu yang telah bersedia membantu dalam menyelesaikan Tugas Akhir ini.

Akhir kata penulis menyampaikan permohonan maaf apabila ada perkataan penulis, baik sengaja maupun yang tidak di sengaja, yang mungkin kurang berkenan ataupun menyinggung di hati pembaca. Namun demikian harapan penulis kiranya laporan ini dapat bermanfaat bagi kita semua.

Palembang, 2021

Penulis

DDoS TCP Flood Attack Prevention System Using Ingress/Egress Filtering Algorithm

Mohammad Cahyadi (09011381621065)
Department of Computer Engineering, Faculty of Computer Science
Sriwijaya University
Email: cahyaditkj@gmail.com

ABSTRACT

DDoS TCP Flood attack is a condition where the attacker exploits the three-way handshaking mechanism of the TCP connection establishment process, where the server will be flooded with requests for SYN packets without being responded by the server. In preventing TCP Flood DDoS attacks, we need a system that will detect the attack pattern and then independently reject packets that indicated as attacks. In this study, the attack prevention system uses a combination of iptables in which the ingress/egress filtering algorithm is applied and Suricata is in charge of rejecting attack packets with known patterns. The packets sent will initially be filtered based on their prefix in iptables, if the packet has a valid prefix then the packet will be analyzed by Suricata which will determine whether the packet is forwarded to the destination IP address or will be rejected, in the end, the captured packet details on the attacker's computer, the prevention system, and the victim's computer will be validated and compared the number of prevention failures. From the results of testing the attack prevention system using the ingress/egress filtering algorithm, in preventing DDoS TCP Flood attacks, the success rate of preventing IP addresses with valid prefixes reaches 93.33%. while prevention for IP addresses with invalid prefixes (Spoofing), ingress/egress filtering managed to prevent all these attack packets.

Keywords: TCP Flood, Intrusion Prevention System, Ingress/Egress Filtering, iptables, suricata

Sistem Pencegahan Serangan *DDoS TCP Flood* Menggunakan Algoritma *Ingress/Egress Filtering*

Mohammad Cahyadi (09011381621065)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: cahyaditkj@gmail.com

ABSTRAK

Serangan *DDoS TCP Flood* adalah kondisi dimana penyerang mengeksploitasi mekanisme *three-way handshaking* dari proses pembentukan koneksi *TCP*, dimana server akan dibanjiri dengan permintaan paket-paket *SYN* tanpa sempat direspon oleh server. Dalam melakukan pencegahan serangan *DDoS TCP Flood*, diperlukan sebuah sistem yang akan mendeteksi pola serangan serangan tersebut dan kemudian secara independen menolak paket yang terindikasi serangan. Pada penelitian ini sistem pencegahan serangan menggunakan kombinasi antara *iptables* yang dalam konfigurasinya diterapkan algoritma *ingress/egress filtering* dan *suricata* yang bertugas menolak paket serangan dengan pola yang telah diketahui. Paket yang dikirim awalnya akan disaring berdasarkan *prefix* di *iptables*, kemudian jika paket tersebut memiliki *prefix* yang sah maka paket akan dianalisis oleh *suricata* yang nantinya akan ditentukan apakah paket tersebut diteruskan ke alamat ip tujuan atau akan ditolak, pada akhirnya *detail* paket yang telah ter-*capture* di komputer penyerang, sistem pencegahan, dan komputer korban akan divalidasi dan dikomparasi jumlah kegagalan pencegahannya. Dari hasil pengujian sistem pencegahan serangan menggunakan algoritma *ingress/egress filtering*, dalam mencegah serangan *DDoS TCP Flood* didapatkan tingkat keberhasilan pencegahan alamat ip dengan *prefix* sah mencapai 93,33%. sedangkan pencegahan untuk alamat ip dengan *prefix* yang tidak sah *(Spoofing)*, *ingress/egress filtering* berhasil mencegah semua paket serangan tersebut.

Kata kunci: *TCP Flood, Intrusion Prevention System, Ingress/Egress Filtering, iptables, suricata*

DAFTAR ISI

Halaman

Halaman Judul i
Halaman Pengesahan ii
Halaman Persetujuan iii
Halaman Pernyataan iv
Kata Pengantar v
Abstract viii
Abstrak ix
Daftar Isi x
Daftar Gambar xii
Daftar Tabel xv
BAB I. PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Tujuan 3
1.3 Manfaat 3
1.4 Rumusan Masalah 3
1.5 Batasan Masalah 4
1.6 Metodologi Penelitian 4
1.7 Sistematika penulisan 5
BAB II. TINJAUAN PUSTAKA 7
2.1 *Distributed Denial of Services (DDoS)* 7
2.2 *TCP Flood Attack* 8
2.3 *Intrusion Detection System (IDS)* 10
2.4 *Intrusion Prevention System (IPS)* 10
2.5 *Ingress & Egress Filtering* 11
2.6 *TCP Flood Dataset* 12
2.7 *Snort* 13
2.8 *Suricata* 14
BAB III. METODOLOGI PENELITIAN 15
3.1 Kerangka Kerja 15
3.2 Topologi Deteksi 17
3.3 Konfigurasi Perangkat Keras dan Sistem operasi 20
3.4 Konfigurasi *Snort* 21
3.4.1 *Network Variable* 21
3.4.2 Decoder 23
3.4.3 Dynamic Load Libraries 23
3.4.4 Preprocessor 24
3.4.5 Ruleset 24
3.4.6 Shared Object Snort Rules 25
3.5 Deteksi Serangan *DDoS* 26
3.6 Ekstraksi Data 29
3.7 Pengenalan Pola dan Klasifikasi Serangan 32
3.8 Perancangan Sistem Ingress/Egress Filtering 34

3.9 Program pencegahan serangan 35
3.9.1 Fungsi Utama 35
3.9.2 Deklarasi *Chain* Ke *Iptables* 35
3.9.3 Memasukkan *Rules* Ke *Chain* 36
3.9.4 Konfigurasi *Suricata* 36
3.9.5 Pembuatan *Rules Drop* Pada Suricata 37
3.9.6 Menjalankan *Suricata* 37
3.10 Menjalankan Program Pencegahan Serangan 38
BAB IV. HASIL DAN ANALISA 40
4.1 Hasil Deteksi Serangan 40
4.2 *Log* Serangan yang Dihasilkan *Snort* 41
4.3 Hasil Ekstraksi Data 42
4.4 Korelasi *Ruleset* dan Alert *Snort* 42
4.5 Korelasi *Raw* Data dan Data Ekstraksi 43
4.6 Pola Serangan DDoS TCP SYNflood 45
4.7 Tingkat Keberhasilan Deteksi Serangan 46
4.8 Iptables Sistem Ingress/Egress Filtering 46
4.9 Serangan IP *Spoofing* Yang Tercegah 47
4.10 *Stats Suricata* Setelah Dilakukan Proses Pencegahan 49
4.11 File Alert 50
4.12 Validasi jumlah serangan yang dicegah 51
4.13 Validasi *detail* serangan 52
4.14 Tingkat Keberhasilan Sistem Pencegahan Serangan 55
BAB V. KESIMPULAN DAN SARAN 56
5.1 Kesimpulan 56
5.2 Saran 57
DAFTAR PUSTAKA 58

DAFTAR GAMBAR

Gambar 2. 1 Statistik Serangan DDoS Yang Terjadi Sampai DenganTahun 2014 [8]..... 8
Gambar 2. 2 Perbandingan Aliran Data Normal Dan Yang Dibanjiri Serangan SYNflood Pada protocol TCP [9]..... 9
Gambar 2. 3 Mekanisme Kerja Mesin Seperti Tools Snort Dalam Mendeteksi Serangan DDoS [13]..... 10
Gambar 2. 4 Mekanisme kerja sederhana mesin dalam melakukan pencegahan serangan berdasarkan input dari network administrator [13]. 11
Gambar 2. 5 Detail Mesin Penyerang Dan Korban Yang Terdapat Pada Dataset Yang Digunakan Pada Penelitian Ini [7]. 13
Gambar 2. 6 Arsitektur Snort Dalam Melakukan Deteksi Serangan Intrusi [16] 14
Gambar 3. 1 Kerangka Kerja Penelitian 17
Gambar 3. 2 Arsitektur Jaringan Pada Dataset [7]..... 18
Gambar 3. 3 Arsitektur Jaringan Pada Penelitian Menggunakan Perangkat Lab..... 18
Gambar 3. 4 Jenis-jenis Serangan Yang Dilakukan Setiap Hari Selama Testbed Berlangsung [7]..... 19
Gambar 3. 5 Konfigurasi Alamat Ip Address Lokal, $HOME_NET Diatur Berdasarkan IP Address Atau Kelas Jaringan Komputer Korban. 22
Gambar 3. 6 Konfigurasi Path Direktori Ruleset Dan Rule-rule Lain Yang Digunakan Sebagai Indikator Bahwa Trafik Tersebut Normal Atau Anomali. 22
Gambar 3. 7 Konfigurasi Daq Yang Berfungsi Sebagai Modul Dropping AFPACKET Pada Snort. 23
Gambar 3. 8 Konfigurasi Direktori Library Preprocessor Sehingga Snort Dapat Mendeteksi Trafik Buruk Yang Melalui Jaringan Secara Default 24
Gambar 3. 9 Konfigurasi Preprocessor Normalisasi Versi Alamat IP Untuk Mode Inline Atau Pencegahan Dan Menonaktifkan Portscan 24
Gambar 3. 10 Konfigurasi Path File Rule Yang Dibuat Secara Manual..... 25
Gambar 3. 11 Rule Untuk Mendeteksi Serangan SYNflood [18]..... 25
Gambar 3. 12 Konfigurasi Rule Threshold..... 25
Gambar 3. 13 Bash Snort Berdasarkan Source Dataset. 26

Gambar 3. 14 Detail Jumlah, Jenis Dan Tipe Paket Yang Berhasil Dibaca Oleh Snort 27
Gambar 3. 15 Low Orbit Ion Canon Pada Serangan Manual 29
Gambar 3. 16 Perintah Dalam Melakukan Fitur Ekstraksi 30
Gambar 3. 17 Aliran Data Feature Extractor Dalam Mengekstrak Data. 30
Gambar 3. 18 Contoh Pola Serangan Dengan Mencocokan Ketiga Data Paket Jaringan 33
Gambar 3. 19 Animasi Algoritma Penyaringan Masuk/Keluar (Hitam = Izinkan, Kuning = Dideteksi, Merah = Drop/Tolak). 34
Gambar 3. 20 Flowchart Fungsi Utama Program Sistem Pencegahan Serangan 35
Gambar 3. 21 Flowchart Predefined-Process membuat Chain Baru Ke IPtables 36
Gambar 3. 22 Flowchart Predefined-Process Memasukkan Rules Ke Chain iptables 36
Gambar 3. 23 Flowchart Predefined-Process Mengedit File Konfigurasi Suricata 37
Gambar 3. 24 Flowchart Predefined-Process Pembuatan Rules Untuk Dropping Paket Serangan 37
Gambar 3. 25 Flowchart Predefined-Process Menjalankan Suricata Ke Sistem 38
Gambar 3. 26 (a) perintah bash pada terminal linux. (b) tampilan program ketika telah dijalankan. 39
Gambar 4. 1 Tampilan Alert Ketika Paket Terdeteksi Sebagai Serangan 40
Gambar 4. 2 Jumlah Paket Yang Terdeteksi Sebagai Serangan 41
Gambar 4. 3 Detail File Log Yang Ditampilkan Menggunakan Wireshark 41
Gambar 4. 4 Hasil Fitur Ekstraksi Data Serangan 42
Gambar 4. 5 Korelasi Rules Dan Alert Dari Snort 43
Gambar 4. 6 Korelasi Raw Data dan Data Ekstraksi Sebagai Validasi. 44
Gambar 4. 7 Pola Serangan DDoS SYNflood Yang Diketahui Dengan Membandingkan Antara Data Serangan Manual dan Serangan Pada Dataset. 45
Gambar 4. 8 Rules ingress/egress filtering yang terpasang pada iptables system. 47
Gambar 4. 9 Detail informasi file suricata.log. 50
Gambar 4. 10 Alert yang dihasilkan suricata Ketika serangan terjadi. 50

Gambar 4. 11 Komparasi total paket yang ter-capture 52
Gambar 4. 12 Korelasi Paket Serangan Pada Komputer Penyerang dan Log Suricata. 53
Gambar 4. 13 Korelasi Detail Paket Serangan dan Alert Suricata. 54

DAFTAR TABEL

Tabel 3. 1 Detail Perangkat Keras Beserta Alamat IP Lokal Dan Publik Yang Ter-capture Pada Dataset 20
Tabel 3. 2 Detail Paket Pada Dataset ISCX 20
Tabel 3. 3 Detail Paket Serangan Pada Dataset ISCX 20
Tabel 3. 4 Detail Konfigurasi Perangkat Keras Yang Dibutuhkan Dalam Penelitian Ini Akan Ditunjukkan Seperti Tabel Berikut: 21
Tabel 3. 5 Paket-paket Yang Dapat Dibaca Snort Dari Dataset UNB Friday Tersebut Meliputi Versi Alamat IP, Protokol Dan Paket Lain. 28
Tabel 3. 6 Pseudocode Program Fitur Ekstraktor 31
Tabel 3. 7 Atribut-Atribut Yang Dihasilkan Oleh Fitur Ekstraktor 32

BAB 1
PENDAHULUAN

Pada bab 1 ini menjabarkan mengenai segala hal yang melatarbelakangi dilakukannya penelitian ini, berdasarkan kasus yang didapatkan dari beberapa literatur penelitian sebelumnya tentang kejahatan *cyber* yang terjadi. Kemudian juga dijelaskan tujuan dan manfaat serta metodologi yang akan dilakukan selama penelitian berlangsung.

1.1 Latar Belakang

Meskipun jumlah proyek *cloud* telah meningkat secara dramatis beberapa tahun lalu, memastikan ketersediaan dan keamanan data proyek, layanan, dan sumber daya masih merupakan masalah penelitian yang penting dan menantang. Serangan *distributed denial of service* (*DDoS*) adalah serangan *cybercrime* kedua yang paling sering terjadi setelah *cracking*. Serangan *DDoS TCP Flood* dapat menghabiskan sumber daya mesin, menghabiskan sebagian besar *bandwidth*, dan merusak perangkat keras mesin dalam waktu singkat [1].

SYNflood bekerja dengan membuat koneksi setengah terbuka ke sebuah *node*. Ketika target serangan menerima paket *SYN* ke *port* yang terbuka, target akan mengirim jawaban berupa paket ber-*flags SYN-ACK* dan mencoba untuk membuat koneksi. Namun, selama *SYNflood*, *Three-way Handsake* tidak pernah selesai karena klien tidak pernah menanggapi *SYN-ACK server*. Akibatnya, "koneksi" ini tetap dalam keadaan setengah terbuka sampai waktunya habis. Serangan *DDoS* tipe ini menyerang pada OSI *Layer* ke empat yaitu *transport* [2]. Dalam kasus ini, *server* menjadi *lost in request*, menghabiskan sumber dayanya dan tidak akan dapat menanggapi permintaan koneksi yang sah [3].

Intrusion Detection System (IDS) adalah *software* atau *hardware* yang melakukan deteksi intrusi dalam sistem informasi. IDS dapat mengklasifikasikan serangan menurut sumber dari apa yang mereka monitor, misalnya, peristiwa terjadinya pencurian data atau serangan yang membanjiri sumber daya pada

jaringan komputer lokal maupun publik. IDS juga dapat mengklasifikasikan berdasarkan metode yang mereka gunakan untuk melakukan deteksi. Secara umum ada dua metode deteksi, yaitu deteksi penyalahgunaan *(Misuse)* dan *anomaly* [4].

Intrusion Prevention System adalah sistem pendekatan baru untuk sistem keamanan jaringan, dengan menggabungkan teknik *firewall* dan *intrusion detection* yang proaktif. Pencegahan serangan yang memasuki jaringan dilakukan dengan cara memeriksa berbagai *log* data dan pencegahan dari sensor pengenalan pola. Ketika serangan diidentifikasi, *intrusion prevention* memblokir dan mencatat data tersebut. *IPS* menggunakan *signature id* untuk mengidentifikasi aktivitas pada lalu lintas jaringan, *host* melakukan deteksi pada paket menuju atau keluar dari jaringan dan akan men-*drop* aktivitas tersebut sebelum terjadi akses ke sumber daya target di jaringan [5].

Teknik untuk mencegah *DDoS* dibagi menjadi dua kategori: (i) Teknik umum, yang merupakan beberapa langkah pencegahan yang biasa digunakan yaitu antivirus, virtualisasi sumber daya mesin dan lain-lain. Yang harus diterapkan oleh masing-masing *server* dan ISP sehingga mereka tidak menjadi bagian dari proses serangan *DDoS*. (ii) Teknik *filtering*, yang meliputi penyaringan masuk, penyaringan keluar, penyaringan paket berbasis *router*, penyaringan IP berbasis catatan *log*, dan lain-lain. Teknik *filtering* yang sangat umum dan terkenal adalah penyaringan *engress / egress.* Teknik-teknik ini mencegah lalu lintas IP *spoofing* masuk ke jaringan yang dilindungi. Pada dasarnya, keknik ini mencegah lalu lintas berbahaya yang ditujukan ke jaringan lokal dan membuang lalu lintas berbahaya yang menuju kejaringan publik [6].

Pada penelitian yang dilakukan oleh A. Sahi, D. Lai, Y. Li, dan M. Diykh, terdapat kesulitan dalam melakukan pencegahan yang berasal dari alamat ip palsu *(IP Spoofing)* sehingga menyebabkan jaringan yang ingin dilindungi tetap terserang oleh *DDoS* [1]. Di penelitian ini, dibuat sebuah program berbahasa pemrograman *python* dan konfigurasi *iptables* yang akan dijalankan untuk mencegah serangan *DDoS* masuk ke dalam jaringan yang dilindungi. Algoritma *ingress/egress filtering* akan diterapkan pada *rules iptables* yang nantinya akan menyaring alamat ip diluar *prefix* yang sah pada *gateway*. *Ingress* akan men-*drop* setiap packet yang berasal

dari *prefix* berbeda dengan *gateway* yang menuju ke jaringan yang dilindungi, sedangkan *egress* akan men-*drop* setiap paket yang berasal dari *prefix* berbeda menuju ke jaringan umum atau eksternal. Di lain isi sistem juga menggunakan suricata untuk men-*drop* paket serangan yang berasal dari alamat ip sah pada jaringan, sehingga jaringan yang dilindungi akan aman dari serangan *DDoS* yang berasal dari ip *Spoofing* maupun dari alamat ip yang sah.

1.2 Tujuan

Tujuan dilakukannya penelitian ini adalah menyelesaikan beberapa masalah yang saat ini masih terjadi dan memenuhi saran dari penelitian sebelumnya yaitu:

1. Melakukan pencegahan terhadap serangan yang telah terdeteksi.
2. Melakukan pencegahan terhadap serangan yang berasal dari IP *Spoofing*.
3. Mengukur seberapa besar tingkat keberhasilan dari algoritma yang digunakan, setelah diterapkan ke sistem pencegahan ini.

1.3 Manfaat

Adapun manfaat yang akan didapat setelah menyelesaikan penelitian ini adalah:

1. Dapat melakukan pencegahan serangan yang masuk ke jaringan lokal
2. Mengurangi tingkat trafik tinggi yang menyebabkan terhambatnya lalu lintas informasi yang dikirim dan diterima pada jaringan
3. Mengetahui pola serangan yang dicegah
4. Mengetahui tingkat keberhasilan dari sistem yang dibuat
5. Sumber daya perangkat keras dan perangkat lunak akan terjaga.

1.4 Rumusan Masalah

Seperti yang telah disampaikan pada penelitian [1] bahwa, tingkat keberhasilan yang didapatkan dalam sistem yang mereka bangun untuk melakukan pencegahan serangan TCP *FLOOD* sudah cukup baik. Namun dari proposal yang mereka ajukan masih memiliki *hole* yang harus diperbaiki kembali. *Hole* tersebut adalah meningkatkan kinerja sistem pencegahan serangan yang dilakukan menggunakan IP *Spoofing* yang tidak termasuk dalam *prefix address* jaringan tersebut. Sehingga rumusan masalah yang dapat diambil adalah “ **Bagaimana cara**

melakukan pencegahan serangan *DDoS* TCP *Flood* yang berasal dari IP *Spoofing* “.

1.5 Batasan Masalah

Dari rumusan masalah diatas, selanjutnya dapat ditentukan batasan masalah yang akan dibahas pada penelitian ini yaitu:

1. Serangan yang digunakan hanya *DDoS TCP SYNflood*.
2. *Dataset* yang digunakan dalam pengenalan berdasarkan hasil *record* Universitas *New Brunswick* yang berstandar *ISCX* dan *capture* data yang dilakukan secara manual.
3. Pola serangan yang digunakan berdasarkan pola pada *log snort*.
4. *Tools* yang digunakan dalam melakukan serangan adalah *DDoS LOIC* dan *hping3*.
5. Sistem pencegahan menggunakan kombinasi *iptables* dan *suricata.*
6. Skenario pengujian sistem dilakukan secara *offline.*

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini melalui beberapa proses seperti berikut:

1. Tahap Pertama (Studi literatur)

   Tahap ini dilakukan setelah masalah yang akan dibahas telah sesuai dan relevan untuk dijadikan sebagai penelitian, dengan membaca artikel atau makalah penelitian yang berhubungan langsung dengan tugas akhir.

2. Tahap kedua (Perancangan Sistem)

   Pada tahapan ini merupakan tahapan mengenai bagaimana membangun dan menerapkan metode pada sistem tugas akhir. Selain itu, apa yang digunakan pada penelitian seperti *hardware* dan *software*, kemudian bagaimana proses konfigurasi ataupun menulis kode untuk penerapan metode pada tugas akhir.

3. Tahap ketiga (Pengujian)

   Tahap ini merupakan tahap pengujian setiap proses perancangan sistem sehingga didapatkan data hasil uji yang sesuai dan tepat dengan algoritma yang digunakan.

4. Tahap keempat (Analisa)

   Tahap ini adalah proses menganalisa data hasil pengujian dengan diterapkan pendekatan tertentu atau membandingkan setiap hasil dengan penelitian sebelumnya, sehingga didapatkan hasil data yang *valid* dimana data tersebut diperoleh dari proses pengujian.

5. Tahap kelima (Kesimpulan dan Saran)

   Tahap ini adalah proses menarik kesimpulan dari analisa dan studi literatur, serta penulisan saran untuk peneliti selanjutnya agar dapat menyelesaikan masalah yang belum terpecahkan pada penelitian ini.

1.7 Sistematika penulisan

Untuk lebih memahami mengenai isi dari laporan tugas akhir ini, maka setiap materi disajikan dengan cara dikelompokkan menjadi sub-sub bab. Sistematika penulisan laporan tugas akhir ini sebagai berikut:

BAB 1 PENDAHULUAN

Pada bab ini menjelaskan mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat yang akan didapat setelah menyelesaikan penelitian.

BAB 2 TINJAUAN PUSTAKA

Ditinjauan pustaka ini berisikan tentang pengertian, istilah, dan contoh-contoh yang diambil dari makalah, buku, serta literatur *review* tentang topik yang menjadi referensi penelitian.

BAB 3 METODOLOGI PENELITIAN

Di bab ini ditunjukkan langkah-langkah percobaan, *pseudocode* yang telah dibuat, serta implementasi perangkat kedalam sebuah jaringan.

BAB 4 HASIL DAN ANALISA

Setelah dilakukan percobaan, maka didapatkanlah hasil yang akan dianalisis pada bab 4 ini. Sehingga mendapatkan titik terang dari penelitian yang dilakukan

BAB 5 PENUTUP

Pada bab 5 ini diberikan kesimpulan dari hasil penelitian dan saran untuk diselesaikan pada penelitian yang akan dilakukan.

DAFTAR PUSTAKA

[1] A. Sahi, D. Lai, Y. Li, and M. Diykh, "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment," *IEEE Access*, vol. 5, no. c, pp. 6036–6048, 2017, doi: 10.1109/ACCESS.2017.2688460.

[2] A. Possibilities and B. Y. Osi, "ATTACK POSSIBILITIES BY OSI LAYER," no. October, 2020.

[3] M. A. Jubair *et al.*, "A Simulation Study of Syn Flood Attack In Cloud Computing Environment A Simulation Study of Syn Flood Attack In Cloud Computing Environment Un Estudio De Simulación Del Ataque De Inundaciones," no. march 2020, pp. 188–197, 2019, doi: 10.4206/aus.2019.n26-1.19/.

[4] N. Nokuthala, P. Mkuzangwe, and F. V. Nelwamondo, "Detection System for Predicting the TCP SYN Flooding Attack," vol. 2, pp. 14–22, 2017, doi: 10.1007/978-3-319-54430-4.

[5] D. Stiawan, A. H. Abdullah, and M. Y. Idris, "The trends of Intrusion Prevention System network," *ICETC 2010 - 2010 2nd Int. Conf. Educ. Technol. Comput.*, vol. 4, pp. 217–221, 2010, doi: 10.1109/ICETC.2010.5529697.

[6] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *Int. J. Distrib. Sens. Networks*, vol. 13, no. 12, 2017, doi: 10.1177/1550147717741463.

[7] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," *ICISSP 2018 - Proc. 4th Int. Conf. Inf. Syst. Secur. Priv.*, vol. 2018-Janua,

no. Cic, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

[8] G. Ramadhan, Y. Kurniawan, and C. S. Kim, “Design of TCP SYN Flood DDoS attack detection using artificial immune systems,” *Proc. 2016 6th Int. Conf. Syst. Eng. Technol. ICSET 2016*, pp. 72–76, 2017, doi: 10.1109/FIT.2016.7857541.

[9] P. S. Kenkre, A. Pai, and L. Colaco, “AISC 327 - Real Time Intrusion Detection and Prevention System,” vol. 1, pp. 405–411, 2015, doi: 10.1007/978-3-319-11933-5.

[10] A. S. Desai, “Real Time Hybrid Intrusion Detection System using Signature Matching Algorithm and Fuzzy-GA,” pp. 291–294, 2016.

[11] Q. Niyaz, W. Sun, A. Y. Javaid, and M. Alam, “A Deep Learning Approach for Network Intrusion Detection System,” 2016, doi: 10.4108/eai.3-12-2015.2262516.

[12] Y. Farhaoui, “Design and implementation of an intrusion prevention system,” *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 675–683, 2017, doi: 10.6633/IJNS.201709.19(5).04.

[13] A. Sawant, “A Comparative Study of Different Intrusion Prevention Systems,” *2018 Fourth Int. Conf. Comput. Commun. Control Autom.*, pp. 1–5, 2018.

[14] N. M. Lanke and C. H. R. Jacob, “Detection of DDOS Attacks Using Snort Detection,” vol. 2, no. 9, pp. 13–17, 2014.

[15] R. Fekolkin, “Intrusion Detection and Prevention Systems: Overview of Snort and Suricata,” no. January 2015, pp. 4–7, 2015, [Online]. Available: https://snort.org/,.

[16] T. T. Oo and T. Phyu, “Analysis of DDoS Detection System based on Anomaly Detection System,” 2014, doi: 10.15242/iie.e0314146.