Deteksi Serangan Syn Flood Pada Server Menggunakan Metode Algoritma K-Nearest Neightbor

M.Fierza Eries Erlangga[1], Nuniek Fahriani[2], Ashr Hafiizh Tantri[3]
[1,2,3]Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammdiyah Surabaya
Jl. Raya Sutorejo No.59, Dukuh Sutorejo, Kec. Mulyorejo, Surabaya, Jawa Timur 60113
e-mail: [1]eriezfierza@gmail.com, [2]nuniekfahriani@ft.um-surabaya.ac.id,
[3]ashr.hafiizh.tantri@um-surabaya.ac.id

Abstrak

Dalam beberapa tahun ini, pengguna internet meningkat pesat dari hari ke hari dapat berdampak pada meningkatnya permintaan akses dan data di sebuah server. Hal itu menjadi tujuan utama para penjahat cyber untuk menyerang sebuah server yang dimana penjahat cyber akan berusaha menyerang server dengan melakukan teknik syn flood, Syn flood sendiri masih tergolong teknik serangan DDOS(Dsitributed Denial Of Service) yang dimana serangan tersebut akan melakukan penolakan layanan dimana penyerang dengan cepat memulai koneksi tanpa menyelesaikan koneksi tersebut sehingga Dengan kondisi seperti itu server akan menghabiskan banyak sumber daya untuk menunggu koneksi yang setengah terbuka dan dapat membuat sistem atau server tidak responsif terhadap lalu lintas yang sah pada server. Pada penelitian ini yang bertujuan untuk mengklasifikasikan informasi layanan pada server yang terinjeksi atau terserang oleh syn flood atau tidak dengan cara menggunakan metode algoritma K-Nearest Neightbor. Algoritma K-Nearest Neighbor menghitung jarak pada setiap fitur yang ada dalam dataset kemudian mengidentifikasi jenis flow berdasarkan dengan mayoritas pada nilai ketetanggaan (nilai k) tertentu. Hasil pengujian pada penelitian ini adalah akurasi sebesar 92,57% dimana nilai k yang ditentukan sesuai default sistem yaitu 5. Nilai k terbaik pada penelitian ini tidak dapat ditentukan karena pengujian yang dilakukan untuk menentukan nilai k mendapatkan hasil dengan perbedaan nilai yang cukup berjauhan. Metode yang diusulkan dapat digunakan dalam mengklasifikasikan informasi layanan pada server yang terindikasi oleh serangan Syn Flood.

Kata Kunci : *Syn Flood, DDOS,DDOS syn flood, K-Nearest Neightbor, Metasploit*

Abstract

In recent years, internet users have increased rapidly from day to day, which can have an impact on increasing demand for access and data on a server. This is the main goal of cyber criminals to attack a server where cyber criminals will try to attack the server by carrying out the Syn Flood technique, Syn Flood itself is still classified as a DDOS (Distributed Denial Of Service) attack technique where the attack will make a service request where the attacker quickly starting a connection without completing the connection so that in such conditions the server will spend a lot of resources waiting for half-open connections and can make the system or server unresponsive to legitimate traffic on the server. In this research, the aim is to classify information services on servers that are injected or attacked by syn flood or not by using the K-Nearest Neighbor algorithm method. The K-Nearest Neighbor algorithm calculates the distance to each feature in the dataset and then identifies the type of flow based on the majority of certain neighborhood values (k values). The test results in this study were an accuracy of 92.57% where the k value determined was according to the system default, namely 5. The best k value in this study could not be determined because the tests carried out to determine the k value obtained results with quite large differences in values. The proposed method can be used to classify information services on servers that are indicated by Syn Flood attacks.

Keyword *: Syn Flood, DDOS,DDOS syn flood, K-Nearest Neightbor, Metasploit*

1. PENDAHULUAN

DDOS *attack* atau *Distributed Denial of Service* merupakan serangan *cyber* dengan cara mengirimkan *fake traffic* atau lalu lintas palsu ke suatu sistem atau server secara terus menerus. Dampaknya, server tersebut tidak dapat mengatur seluruh *traffic* sehingga menyebabkan *down [5]]*. DDoS(Syn Flood) tidak seperti jenis serangan DDoS lainnya, serangan DDoS SYN Flood tidak dimaksudkan untuk menggunakan semua memori host, melainkan untuk menghabiskan cadangan koneksi terbuka yang terhubung ke port, dari alamat IP individu dan seringkali palsu. Banjir SYN sering disebut serangan "setengah terbuka" karena jenis serangan DDoS ini bermaksud untuk mengirim pesan SYN secara singkat ke port, membiarkan koneksi yang tidak aman terbuka dan tersedia, dan sering mengakibatkan server crash total. Target serangan DoS attack bisa ditujukan ke berbagai bagian jaringan, bisa ke routing,devices, web, electronicmail, atau serverDomain Name System. Server adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer *[1]*.

Sistem informasi terpusat seperti pada cloud computing, sangat rawan terhadap berbagai ancaman keamanan jaringan seperti serangan DOS, SYN flood, maupun serangan lainnya (Sahren, 2021). Menurut Khalaf, et al. (2019) dan Lukman & Suci Melati (2020), serangan DoS yang sering dilakukan pada jaringan cloud diantaranya seperti UDP flood, SYN flood, ping of death, smurf, HDoS, dan XDoS. Berdasarkan masalah yang terdapat pada fakta-fakta tersebut, teori pada penelitian sebelumnya yang dilakukan oleh Pilli, et al. (2010) dan Fathoni, Fitriyani & Nurkahfi, (2016) menyatakan bahwa solusi untuk mengungkap masalah keamanan jaringan yang terjadi yaitu melalui forensik jaringan *[6]*.

Mendeteksi Serangan SYN Flood dilakukan dengan menggunakan beberapa salah satunya dengan metode EMD(Earth Mover's 2 Distance). Metode EMD(Eart Mover's Distance) dilakukan dengan cara mengubah rute secara instan node dalam SDN(Software Defined Network) skala besar. metode ini juga membutuhkan waktu sedikit lebih lama dikarenakan mengubah node dalam SDN(Software Defined Network) yang berskala besar [7].

Namun, pada penelitian ini penulis mengusulkan untuk menggunakan metode K-Nearest Neightbor untuk mendeteksi serangan Ddos SYN Flood. Kelebihan metode ini yaitu dengan menerapkan metode KNN kita dapat mengklasifikasikan data berdasarkan ukuran kesamaan. Klasifikasi dilakukan berdasarakan data pembelajaran dengan objek yang terdekat dari data pembelajaran tersebut.[8]

Oleh karena itu penelitian ini dilakukan untuk mendeteksi adanya serangan ddos syn flood yang ditujukan untuk server ataupun web server. Dengan adanya penelitian ini diharapkan dapat mencegah atau mengatasi serangan ddos syn flood dan dapat menghindari kerugian akibat serangan ddos syn flood.

2. METODE PENELITIAN

Penelitian ini menerapkan metode kualitatif atau studi kasus dikarenakan dilakukan dengan kondisi memahami fenomena yang kompleks dalam konteks yang nyata. Metode peneletian kualitatif adalah sebagai prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang dapat diamati sebagai mana adanya. Studi kasus adalah memahami suatu kasus, orang-orang tertentu atau situasi secara mendalam (Creswell, 2014).

- **JENIS DATA**
  Sumber data penentuan sumber data ini terdapat dua buah data yang terkumpul oleh penulis antara lain :

Data primer : yaitu data yang utama dalam penelitian ini, yang meliputi jumlah server yang akan diuji dengan serangan ddos syn flood dan pada saat serangan tadi terjadi penulis akan mencoba mendeteksi serangan tersebut dengan metode KNN atau K-Nearest Neightbor

Data sekunder : yaitu data yang mendukung terhadap data primer. Data sekunder ini akan di peroleh dari server mengenai ketahanan server menahan serangan ddos syn flood yang dilakukan oleh penulis

- **PENGUMPULAN DATA**

Pada Penelitian ini penulis menggunakan 2 metodepengumpulan data:

1. **Obseervasi :** Teknik pengumpulan data yang dilakukaan melalui sesuatu pengamatan, dengan disertai pencatatan-pencatatan terhadap keadaan
   atau prilaku objek sasaran.

2. **Questioner :** adalah "suatu daftar yang berisikan rangkaian pertanyaan mengenai suatu masalah/bidang yang akan diteliti".3 Sementara menurut S.
   Nasution, kuesioner atau yang sering disebut dengan angket adalah "daftar pertanyaan yang didistribusikan untuk di isi dan dikembalikan/dijawab dibawah pengawasan peneliti

- **PENGOLAHAN AWAL DATA**

Pengolahan data dalam penelitian ini menggunakan teknik KNN atau K-Nearest Neightbor melibatkan serangkaian langkah-langkah untuk mempersiapkan & memproses data yang akan diuji sebelum dilakukannya pengujian serangan dengan menggunakan teknik syn flood. Beberapa langkah pengolahan awal data yang dapat dilakukan sebagai berikut :

1. Mempersiapkan hosting & domain untuk mendapatkan server yang akan diuji
2. Mempersiapkan tools ddos syn flood yang nantinya akan digunakan untuk menyerang server yang sudah dipersiapkan
3. Mempersiapkan server & apa saja yang dibutuhkan untuk menunjang dilakukannya uji coba serangan ddos menggunakan teknik syn flood
4. Menerapkan metode KNN atau K-Nearest Neightbor untuk mendeteksi serangan ddos syn flood yang dilakukan oleh penulis.

- **MODEL/METODE YANG DIUSULKAN**

Dalam metode ini menggunakan teknik KNN atau K-Nearest Neightbor , penulis mengusulkan metode KNN atau K-Nearest Neightbor untuk mencapai tujuan penelitian . Berikut adalah penjelasan mengenai metode yang diusulkan:

1. **K-Nearest Neightbor :** penulis mengusulkan untuk menggunakan metode K-Nearest Neightbor untuk mendeteksi serangan Ddos SYN Flood. Kelebihan metode ini yaitu dengan menerapkan metode KNN kita dapat mengklasifikasikan data berdasarkan ukuran kesamaan. Klasifikasi dilakukan berdasarakan data pembelajaran dengan objek yang terdekat

dari data pembelajaran tersebut. Metode yang diusulkan ini memanfaatkan klasifikasi data dalam mendeteksi adanya serangan ddos syn flood .

- **EKSPERIMEN & PENGUJIAN MODEL/METODE**

Dalam konteks peneletian ini menggunakan metode KNN atau K-Nearest Neighbor, eksperimen dan pengujian metode menjadi langkah yang penting untuk menguji keefektifan dan keakuratan metode yang diusulkan. Berikut adalah beberapa langkah yang dapat dilakukan dalam eksperimen dan pengujian metode ini:

Tahap Persiapan:

- Mengumpulkan data serangan SYN flood yang telah terjadi sebelumnya.
- Mengumpulkan data lalu lintas jaringan normal.
- Identifikasi fitur-fitur yang relevan untuk deteksi serangan SYN flood.
- Melakukan preprocessing data, seperti normalisasi dan ekstraksi fitur.

Tahap Pembangunan Model:

- Membagi dataset menjadi data latih (training data) dan data uji (testing data).
- Melatih model K-Nearest Neighbor menggunakan data latih.
- Validasi model menggunakan data uji dan melakukan penyetelan parameter (misalnya, nilai k).

Tahap Implementasi:

- Mengimplementasikan model deteksi serangan SYN flood ke dalam server yang akan diproteksi.
- Mengintegrasikan algoritma K-Nearest Neighbor ke dalam sistem server untuk memantau lalu lintas jaringan secara real-time.

Tahap Deteksi Serangan:

- Menerima lalu lintas jaringan yang masuk ke server.
- Mengumpulkan informasi tentang paket yang diterima, seperti jumlah SYN packet, SYN-ACK packet, dan RST packet.
- Menggunakan model K-Nearest Neighbor untuk menganalisis data paket dan mendeteksi serangan SYN flood.

Tahap Penanganan Serangan:

- Jika serangan SYN flood terdeteksi, mengambil tindakan mitigasi yang sesuai.
- Contoh tindakan mitigasi dapat mencakup pemblokiran IP sumber yang mencurigakan atau menerapkan mekanisme penanggulangan serangan seperti SYN cookies.

Tahap Evaluasi:

- Melakukan evaluasi performa model deteksi menggunakan metrik seperti akurasi, presisi, recall, dan F1-score.
- Menganalisis kelebihan dan kekurangan dari pendekatan yang digunakan.

- Menyarankan perbaikan atau pengembangan lebih lanjut untuk meningkatkan kinerja deteksi serangan SYN flood.

3. HASIL DAN PEMBAHASAN

Evaluasi dan validasi data merupakan langkah penting dalam penelitian untuk memastikan keakuratan, keandalan, dan validitas data yang telah dikumpulkan. Berikut adalah beberapa langkah yang dapat dilakukan dalam evaluasi dan validasi data:

- Melakukan evaluasi performa model deteksi menggunakan metrik seperti akurasi, presisi, recall, dan F1-score.
- Menganalisis kelebihan dan kekurangan dari pendekatan yang digunakan.
- Menyarankan perbaikan atau pengembangan lebih lanjut untuk meningkatkan kinerja deteksi serangan SYN flood.

4. KESIMPULAN

Penelitian ini mengusulkan penggunaan K-NN untuk mendeteksi serangan SYN Flood. Hasil penelitian menunjukkan akurasi sebesar 92,57%. Kesimpulannya adalah bahwa metode K-NN dapat digunakan untuk mendeteksi serangan SYN Flood dan mengambil tindakan mitigasi yang sesuai.

UCAPAN TERIMAKASIH

Penulis menyampaikan terima kasih kepada pihak-pihak yang telah mendukung penelitian ini.

DAFTAR PUSTAKA

1. https://www-netscout-com.translate.goog/what-is-ddos/syn-flood-attacks?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc
2. https://www.dicoding.com/blog/apa-itu-server/
3. https://www.researchgate.net/publication/343203704_Analisa_Sistem_Identifikasi_DDoS_Menggunakan_KNN_Pada_Jaringan_Software_Defined_NetworkSDN
4. *https://publikasi.mercubuana.ac.id/index.php/format/article/download/18000/pdf*
5. https://www.elitery.com/articles/apa-itu-ddos/
6. https://e-journal.hamzanwadi.ac.id/index.php/edumatic/article/download/6466/pdf
7. https://publications.waset.org/10009068/an-earth-movers-distance-algorithm-based-ddos-detection-mechanism-in-sdn
8. https://www.researchgate.net/publication/343203704_Analisa_Sistem_Identifikasi_DDoS_Menggunakan_KNN_Pada_Jaringan_Software_Defined_NetworkSDN
9. https://repository.mercubuana.ac.id/73025/1/41518210001%20-%20MUCHAMAD%20OKTARIN%20JATMIKA%20-%2001%20Cover.pdf
10. https://www.neliti.com/publications/374488/tcp-syn-flood-dos-attack-prevention-using-spi-method-on-csf-a-poc