JURNAL ILMIAH ELEKTRONIKA DAN KOMPUTER, Vol.14, No.2, Desember 2021, pp. 268 - 277
p-ISSN : 1907-0012 (print)
e-ISSN : 2714-5417 (online)
http://journal.stekom.ac.id/index.php/elkom

IMPLEMENTASI APLIKASI *SOFTWARE NATURAL NETWORK* MENDETEKSI TINGKATAN SERANGAN DDOS PADA JARINGAN KOMPUTER

Etza Nofarita[1]
[1]Teknik Komputer/Akademi Manajemen dan Informatika (AMIK) KOSGORO
Jl. RSDK No. 340 Koto Panjang Kota Solok, Sumatera Barat,e-mail: etzanovarita@gmail.com

ARTICLE INFO

Article history:

Received 22 Oktober 2021
Received in revised form 24 Oktober 2021
Accepted 24 Oktober 2021
Available online 1 Desember 2021

ABSTRACK

Security issues of a system are factors that need to be considered in the operation of information systems, which are intended to prevent threats to the system and detect and correct any damage to the system. Distributed Denial of Services (DDOS) is a form of attack carried out by someone, individuals or groups to damage data that can be attacked through a server or malware in the form of packages that damage the network system used. Security is a mandatory thing in a network to avoid damage to the data system or loss of data from bad people or heckers. Packages sent in the form of malware that attacks, causing bandwidth hit continuously. Network security is a factor that must be maintained and considered in an information system. Ddos forms are Ping of Death, flooding, Remote controled attack, UDP flood, and Smurf Attack. The goal is to use DDOS to protect or prevent system threats and improve damaged systems. Computer network security is very important in maintaining the security of data in the form of small data or large data used by the user.

Keywords: *Distributed Denial of Service, Natural Network, Aplikasi Matlab*

Abstrak

Masalah keamanan suatu sistem merupakan faktor-faktor yang perlu diperhatikan dalam pengoperasian sistem informasi, yang dimaksudkan untuk mencegah ancaman terhadap sistem dan mendeteksi serta memperbaiki setiap kerusakan pada sistem. Distributed Denial of Services (DDOS) adalah suatu bentuk serangan yang dilakukan oleh seseorang, individu atau kelompok untuk merusak data yang dapat diserang melalui server atau malware berupa paket-paket yang merusak sistem jaringan yang digunakan. Keamanan merupakan hal yang wajib dalam sebuah jaringan untuk menghindari kerusakan sistem data atau kehilangan data dari orang jahat atau hecker. Paket yang dikirim berupa malware yang menyerang, menyebabkan bandwidth terkena terus menerus. Keamanan jaringan merupakan faktor yang harus dijaga dan diperhatikan dalam sebuah sistem informasi. Bentuk Ddos adalah Ping of Death, banjir, serangan remote control, banjir UDP, dan Serangan Smurf. Tujuannya adalah menggunakan DDOS untuk melindungi atau mencegah ancaman sistem dan memperbaiki sistem yang rusak. Keamanan jaringan komputer sangat penting dalam menjaga keamanan data baik data kecil maupun data besar yang digunakan oleh pengguna.
Kata Kunci: Distributed Denial of Service, Natural Network, Aplikasi Matlab

Received October 22, 2021; Revised October 24, 2021; Accepted October 24, 2021

1. Pendahuluan

Keamanan jaringan sangat penting Bagi sebuah proses system informasi. Tujuannya untuk menjaga atau mencegah ancaman system serta memperbaiki system yang rusak. Keamanan jaringan computer merupakan hal yang sangat penting dalam menjaga keaman data baik dalam bentuk data kecil atau data besar bagi para penggunakan system. Bagi para pemakai harus menjaga data dari berbagai serangan seperti orang orang yang tidak berhak, pada Sistem deteksi penyusup jaringan pada ahkir akhir ini Sebagai system keamaan pada saat sering di sitem dilakukan oleh administrator. *Denial of service* adalah bentuk dari serangan SYN *flooding attack* yang berkembang 22 tahun yang lalu yaitu tahun 1996 yang mendaptkan Kekurangan kelemahan pada pada *protocol* Transmission *control protocol* (TCP). Setelah serangan ini dikembangkan oleh para ahli sehingga menghasilkan kelemahan pasa system operasi.

2. Tinjauan Pustaka

Pada keamanan jaringan ini menghasikan *system,* Pada system ini tidak sapat membantu crash. Jenis alat bantu yang dipakai dalam DDos Bonk, LAND, *smurf, snork, winnuke* dan *teardrop*. Hal ini menyebabkan banjir Berbagai macam penelitian yang dilakukan serangan DDos pada akhir akhir ini serangan cracker sangat meningkat meningkat. Dari berbagai situs menjelaskan bahwa game aplikasi (Prmainan yang paling banyak terkena serangan Hal ini menyebabkan banjir Berbagai macam penelitian yang dilakukan serangan DDos pada akhir akhir ini serangan cracker sangat meningkat meningkat. Dari berbagai situs menjelaskan bahwa game aplikasi (Prmainan yang paling banyak terkena serangan Hal ini menyebabkan banjir Berbagai macam penelitian yang dilakukan serangan DDos pada akhir akhir ini serangan cracker sangat meningkat meningkat. Dari berbagai situs menjelaskan bahwa game aplikasi (Prmainan yang paling banyak terkena serangan serangan (DDOS).Dari data yang diperoleh berupa Akamay Report menjelaskan sebesar 79% total serangan pada tahun 2017 triwulan IV ditemukan dalam game permainan. Selain dalam game juga merusak aplikasi komunikasi internet sebesar enam persen dari awal 3 persen. Akibat serangan ini jaringan tidak dapat diproses dan dicari sehingga user kehilangan data yang dimiliki. Serangan ini dilakukan oleh lebih alamat protocol. Jika dilihat dari traffic banyak serangan yang terjadi baik secara sembunyi sembunyi maupun langsung.

Bagian kecil yang berdampak pada *network security.* Banyak cara yang dapat dilakukan oleh user dalam meningkatkan keamanan jaringan baik dengan meningkatkan atau membuat sebuah feriwel, memakai system 7layer menggunakan *network security.* Pada penelitian ini menggunakan prinsip kerja ke jaringan, switch port security dengan mengandalkan LAN. Manfaat penelitian ini adalah melihat system yang digunakan kira kira sistim ini mampu menghadang serangan serta bisa dipakai di berbagai tempat Oris Krianto Sulaiman(2016). Serangan Ddos setiap perkembangan zaman semakin meningkat dilihat dari isi, pembagian serta pembiayaan semakin tinggi dalam sebuah ruang lingkup yang besar. Tujuan dari penelilian yang diamati dengan melaksanakan sebuah pemahaman dan menganalisi agar bisa mengantisipasi serangan yang terjadi. Sistem ini mengguunkan *natural network* menggunakan fungsi (FMAW) Sebagai alat pendeteksi. Pada penemuan ini memakai CAIDA DDoS Attack 2007 cara sendiri.Hasil akhir dalam penelitian ini mendapatkan 3 pembagian hasil ahir serangan yang terjadi(Rendah sedang da tinggi serangan yang terjadi pada Ddos. Nilai angka yang didapatkan sebanyak 90,52%. Diharapkan dengan penemuan ini bisa menjadi pedoman dalam peramalan serangan. Arif Wirawan Muhammad (1), Imam Riadi (2), Sunardi (3) (2017).

Menurut (Muhammad & Riadi, 2017) Ada cara dalam penanggulangan dalam mendeteksi serangan DDos, hal ini dilihat dari dari berbagai perhitungan menggunakan rumus matematika dan pencarian *neural network* penentu jumlah serangan yang terjadi. Pada penelitian dan pengujian ini mendapatkan hasil jika serangan itu terbagi atas tiga bagian yaitu kecil, sedang dan besar. Tujuan penelitian ini yaitu mendeteksi dengan cara melakukan pendekatan serta cara cara penanggulangan serangan yang terjadi. Hasil akhir dari penelitian ini berupa ilustrasi dan ramalan yang terjadi pada jaringan computer.

Menurut (Kato & Klyuev, 2014) penelitian yang dilakukan menggunakan teknik penyelesaian masalah dengan menggali system analisa dengan mempelajari dan mengambil kelebihan dari system mesin learning dan mempelajari bentuk pola serangan yang terjadi. Bentuk penelitian yang dilakukan berupa menganalisa system paket yang sering digunakan dalam data baik berupa internet maupun system yang bisa mendeteksi (SVM).

p-ISSN: 1907-0012 e-ISSN : 2714-5417

Akibat yang timbul dari Serangan Daniel of service (Dos Attack) pertama menghabiskan resources(sumber) Melemahkan satu layanan yang digunakan dalam pemakaian resource sehingga mesin computer yang kena Serangan kehabisan resource mengakibatkan hang yang kedua merusak dan mengubah konfigurasi sehingga kita tidak bisa menggunakan jaringan tersebut dan yang ketiga kerusakan fisik sehingga mengubah komponen computer dan merusak komponen fisik. Sebaiknya pada keamanan jaringan kita harus menjaga keamanan fisik, karena keamanan fisik merupakan komponen utama dalam melawan beberapa serangan yang terjadi pada *Daniel of service*.

(Irsyad, 2015), Dalam mencegah serangan pada penelitian ini maka peneliti harus memikirkan teknik yang paling akurat dalam menjaga serangan DDos. Proses yang dilakukan dalam penelitian ini berupa system perhitungan matematika menggunakan prinsip (MCA). Sistem yang dipakai dengan mempelajari tampilan hasil nyata. Menggunakan data berupa peninjauan dengan beberapa metode yang dipakai bisa algoritma pencarian dengan menghitung semua nilai yang terjadi pada serangan yang terjadi saat serangan.

Langkah langkah dalam mengatasi serangan DDos 1. Membuat identifikasi serangan akan tampat pada saat melihat server. 2 Tetap menggunakan parameter network dengan cara memperbesar bandwith 3. Memanggil hosting provider ISP mereka melacak serangan melewati IP dalam system 4. Memanggil DDos jika tidak berhasil. Berdasarkan hasil penelitian terdahulu yang sudah dijelaskan makan diharapkan peneliti bisa membuat dan menentukan tingkatan seranagn DDos menggunakan Natural Network. Bentuk serangan terdistribusi DDoS "banyak ke satu" yang membuat serangan ini lebih sulit untuk dicegah. Sebuah serangan DDoS terdiri dari empat elemen, seperti yang ditunjukkan pada Gambar 1. Empat komponen dari serangan DDoS antara lain penyerang, program kontrol utama, *daemon* serangan/*bots*, dan korban. Pertama, melibatkan korban, yaitu *host* target yang telah dipilih untuk menerima beban serangan. Kedua, melibatkan kehadiran agen serangan (*daemon*) yaitu program *agent* yang melakukan serangan secara langsung terhadap korban sasaran. *Daemon* biasanya ditempatkan di komputer inang/perantara. Instalasi *daemon* pada komputer inang mengharuskan penyerang untuk mendapatkan akses dan berhasil menyusup ke komputer yang menjadi inang *daemon*. Komponen ketiga dari serangan DDoS adalah program kontrol utama. Tugasnya adalah untuk mengkoordinasikan serangan. Akhirnya, ada penyerang yang menjadi aktor utama di balik serangan DDoS. Penyerang menginisiasikan serangan dengan menggunakan program kontrol utama di belakang layar. Berikut ini adalah langkah-langkah yang terjadi pada serangan terdistribusi :

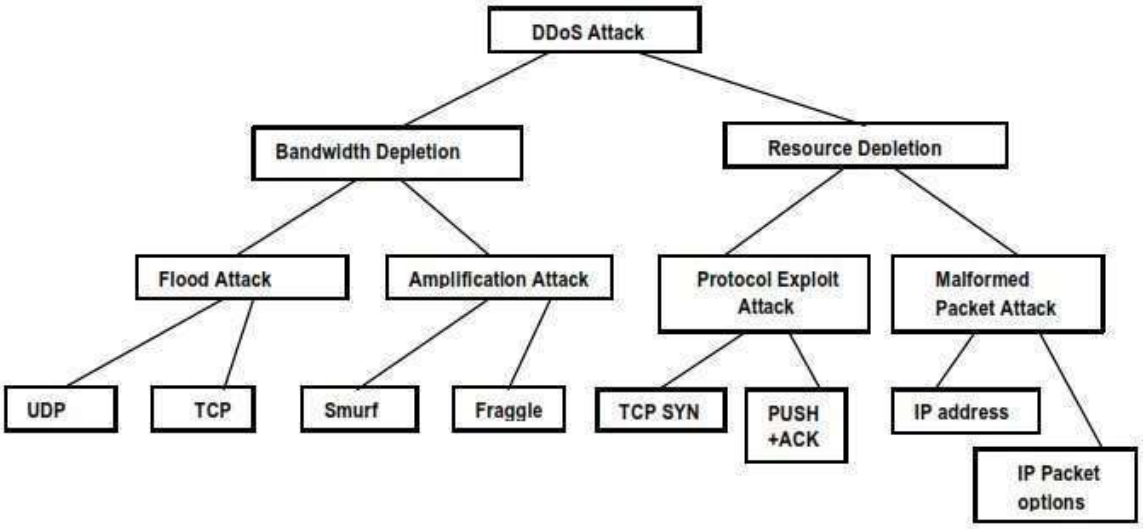
1. Penyerang mengirimkan perintah “eksekusi” yang berupa pesan ke program kontrol utama.
2. Program kontrol utama menerima pesan berupa perintah "eksekusi" dan kemudian menyebarkan perintah penyerangan untuk tiap *daemon* serangan yang berada di bawah kendalinya.
3. Begitu menerima perintah serangan, *daemon* serangan memulai serangan terhadap korban.

Meskipun tampaknya pelaku utama serangan DDoS hanya melancarkan aksinya dengan mengirim perintah eksekusi, namun sebenarnya dia benar-benar harus melakukan perencanaan demi serangan DDoS yang berhasil. Penyerang harus menyusup semua *host* komputer dan jaringan di mana para *daemon* harus terpasang. Penyerang harus mempelajari topologi jaringan target dan mencari celah keamanan.

Melanjutkan dalam menghidupkan sistem tanpa memperhatikan siapa yang menggunakan sistem ini. Tujuan nya untuk memaksimalkan serangan agar bisa tersambung ke server

1. Selalu melakukan update secara terus menerus dalam melihat serangan yang masuk kedalam sebuah server. Untuk mengantisipasi bloc semua ip adress yang masuk.
2. Membagi jalan agar dapat memperkecil serangan yang terjadi pada komputer.
3. Memakai patch agar sistem selalu mengantisipasi serangan yang masuk ke server(Dharma, 2014).

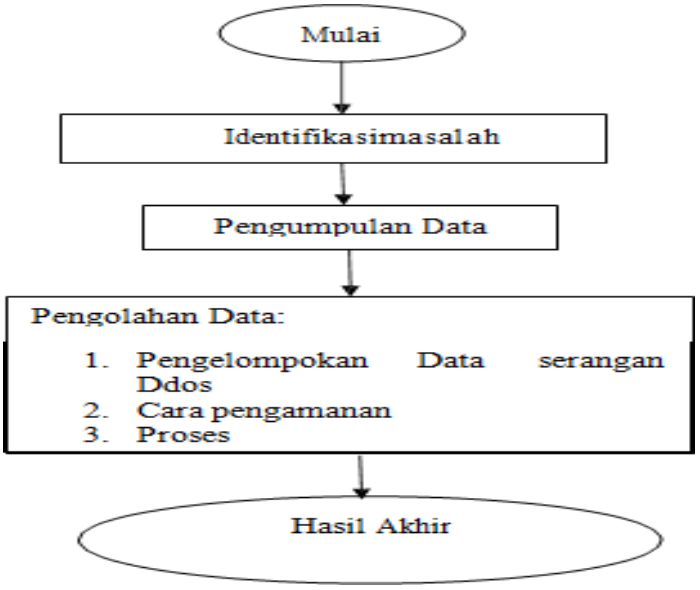
Macam macam serangan Ddos banyak pembagian nya, Cara serangan terjadi berbeda beda sesuai dengan metode masing masing. Pembagian Ddos Menurut (Prasad, Reddy, & Rao, 2014)



Gambar 1. Klasifikasi Serangan DDoS

3. Metodelogi Penelitian

Desain penelitian merupakan sebuah langkah untuk mendaptkan gambaran informasi yang berhubungan dengan serangan DDos pada sebuah data. Dari pengamatan awal didapatkan hipotesis untuk memecahkan masalah yang perlu dipecahkan seperti yang telah disinggung secara garis besar pada bab pendahuluan. Masalah – masalah tersebut adalah :



Gambar 2. Desain Penelitian

4. Hasil dan Pembahasan

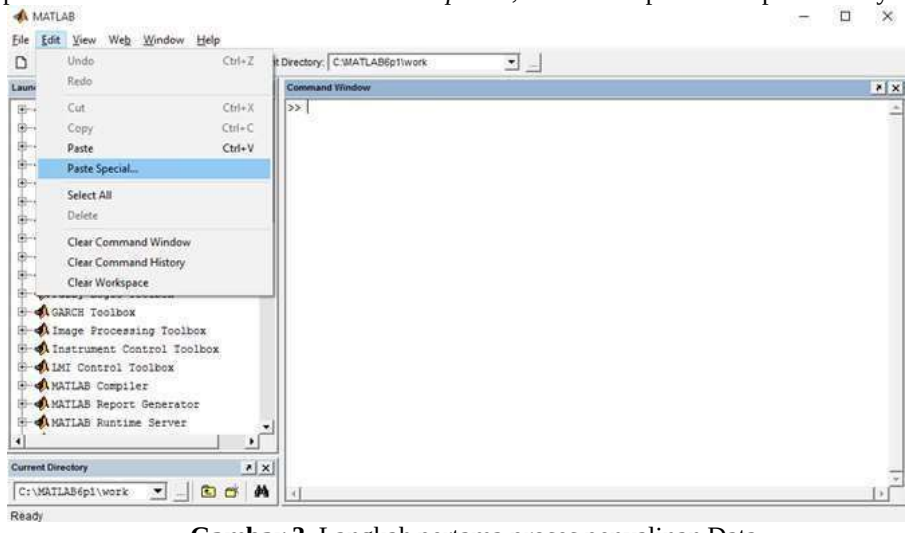
Pada pembahasan ini menggunakan data yang telah di dapatkan dengan panjang dataset sebesar 2500 dengan 5 kriteria, 4 Kriteria akan dijadikan sebagai input sebuah data dan 1 Kriteria akan dijadikan sebagai Target dari sebuah data, berikut data yang akan dipergunakan :

p-ISSN: 1907-0012 e-ISSN : 2714-5417

count	srv_cou	t_host_	host_srv	label
1	5	153	126	normal
1	4	163	128	normal
1	1	173	125	normal
1	2	183	129	normal
4	4	193	87	normal
1	1	203	120	normal
2	10	213	92	normal
9	9	223	102	normal
2	2	233	111	normal
6	6	243	121	normal
1	1	253	123	normal
1	1	255	125	normal
1	3	255	135	normal
1	1	255	145	normal
1	1	1	1	ffer_overflow
1	1	10	153	normal

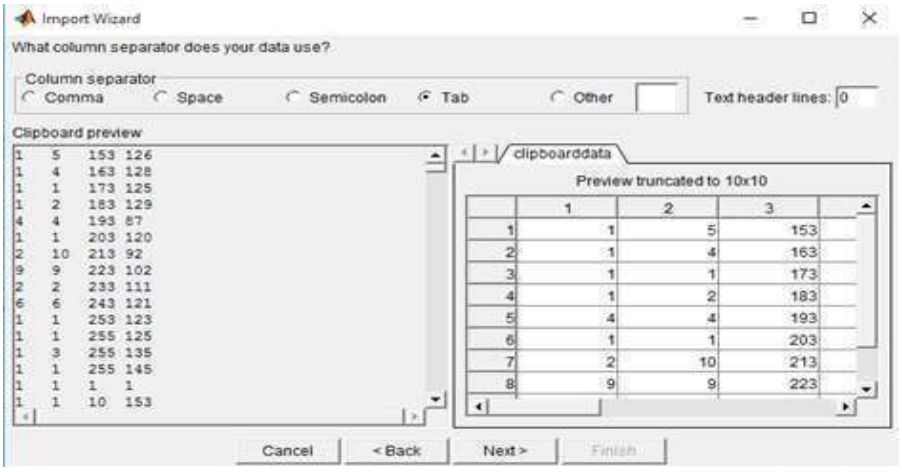
Data yang telah diperoleh akan dijadikan sebuah variable untuk diproses lebih lanjut, berikut langkah-langkah yang akan dilakukan:

1. Proses penyalinan data :
   Proses penyalinan data dilakukan dengan cara mengklik tombol tab *home edit* yang berada pada aplikasi Matlab serta memilih fitur *Paste Special*, berikut tampilan awal proses Penyalinan data :



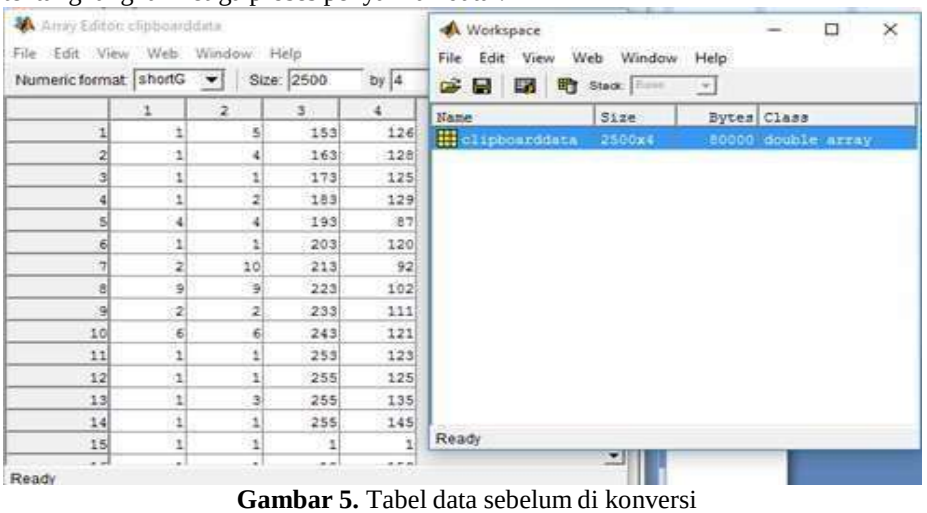
Gambar 3. Langkah pertama proses penyalinan Data

Setelah langkah pertama dilakukan, maka akan muncul berbagai pilihan yang tersedia pada *column separator*, *column separator* bertujuan untuk menentukan format dari sebuah data yang telah di salin. Berikut tampilan dari langkah kedua proses penyalinan data :



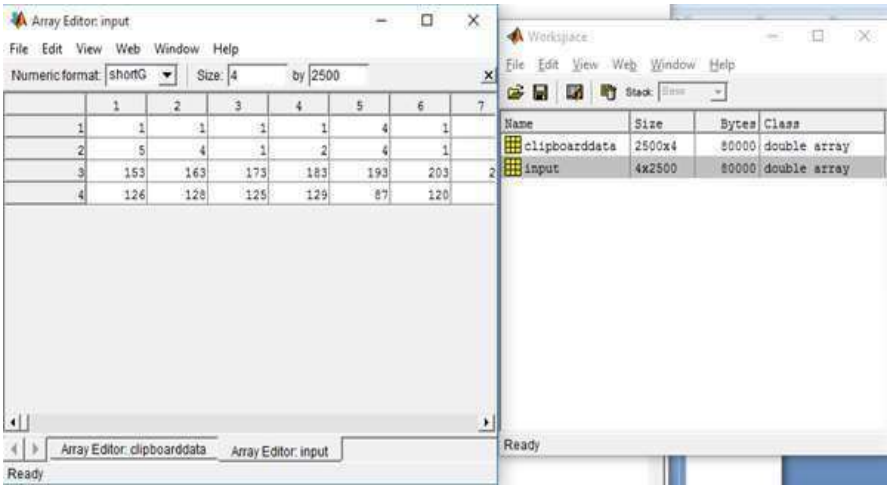
Gambar 4. Langkah kedua proses penyalinan Data

Proses penyalinan ini akan dibuatkan sebuah folder data dengan nama '*clipboarddata*' untuk menyimpan sebuah data bersifat *temporary* atau sementara. Setelah folder data telah tampil langkah berikut nya adalah proses penyalinan data ke folder data baru yang hendak digunakan, dikarenakan pada folder *temporary* tersebu jika tertimpah atau tersisip data lain maka data sebelumnya akan hilang. Pada langkah ketiga dari tahap penyalinan data, data yang disalin sudah tersedia namun belum dapat digunakan pada metode *neural network* dikarenakan data yang disalin akan berbaris secara vertical ke bawah sedangkan *neural network* akan membaca data dengan cara horizontal ke kanan sesuai dengan panjang data yang telah ditentukan. Untuk menyalin sebuah data dari folder *temporary* serta mengubah barisan data kebentuk horizontal panjang kanan dapat menggunakan rumus pada command promt yang telah disedikan oleh aplikasi matlab tersbut, dengan cara " *Tentukan nama folder yang diingkan* = nama folder temporary'; ". Tanda (') pada rumus tersebut adalah tanda pembalik dari data tersebut.
Berikut gambar tentang langkah ketiga proses penyalinan data :



Gambar 5. Tabel data sebelum di konversi

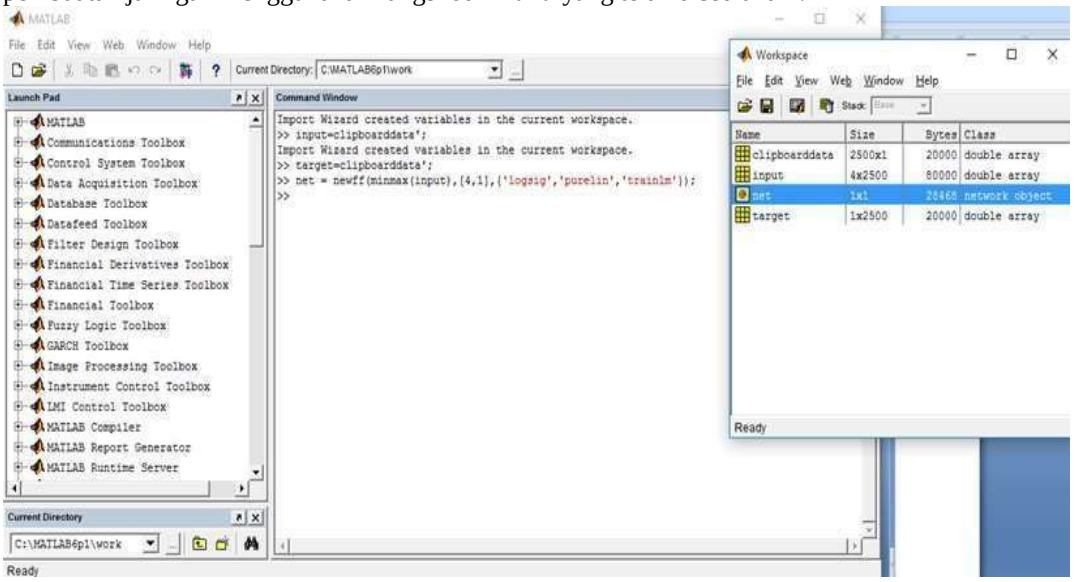
p-ISSN: 1907-0012 e-ISSN : 2714-5417



Gambar 6. Tabel data setelah dilakukan konversi

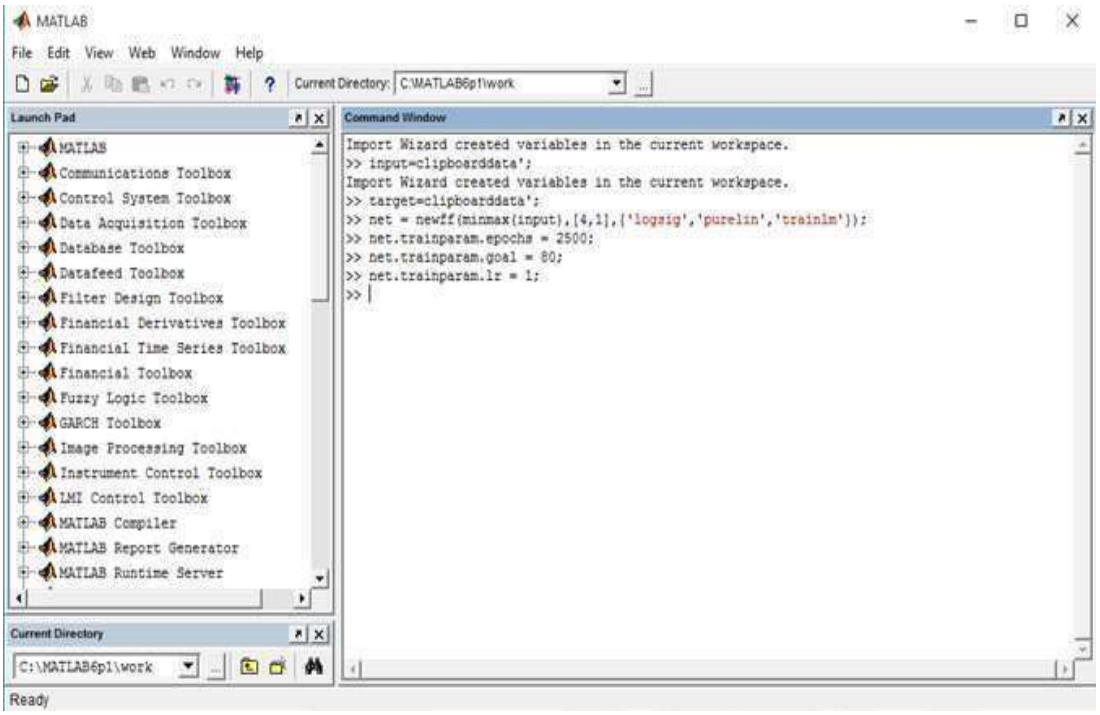
2. Proses pembuatan Neural Network :

Tahapan selanjutnya adalah membuat sebuah jaringan Neural Network dengan menggunakan fungsi *command* yang telah disediakan oleh aplikasi Matlab, berikut gambaran tentang cara pembuatan jaringan menggunakan fungsi *command* yang telah disediakan :



Gambar 7. Pembuatan jaringan *Neural Network*

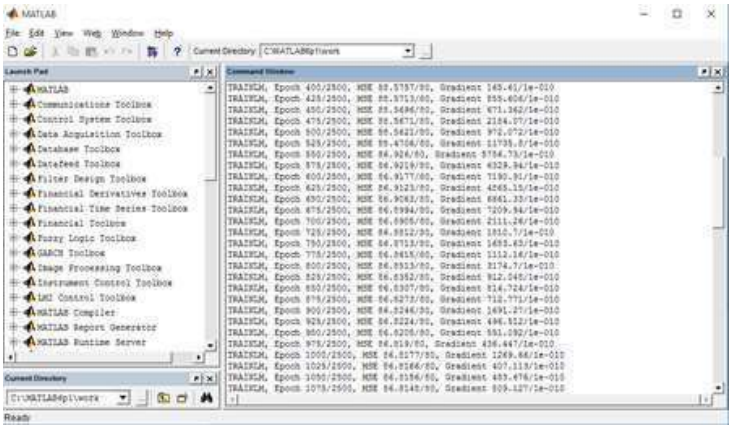
Setelah pembuatan jaringan, maka selanjutnya menentukan kriteria-kriteria yang akan diproses lebih lanjut oleh jaringan Neural Network. Untuk memnentukan kriteria dan fungsi tersebut menggunakan *command* yang disediakan oleh aplikasi Matlab, fungsi ini akan menentukan panjang sebuah data serta nilai goal yang akan dicapai pada saat proses simulasi sedang berjalan. Berikut gamar mengenai penentuan kriteria dan fungsi pada jaringan *Neural Network* :



Gambar 8. Penentuan kriteria dan fungsi pada *Neural Network*

Hasil *Output*

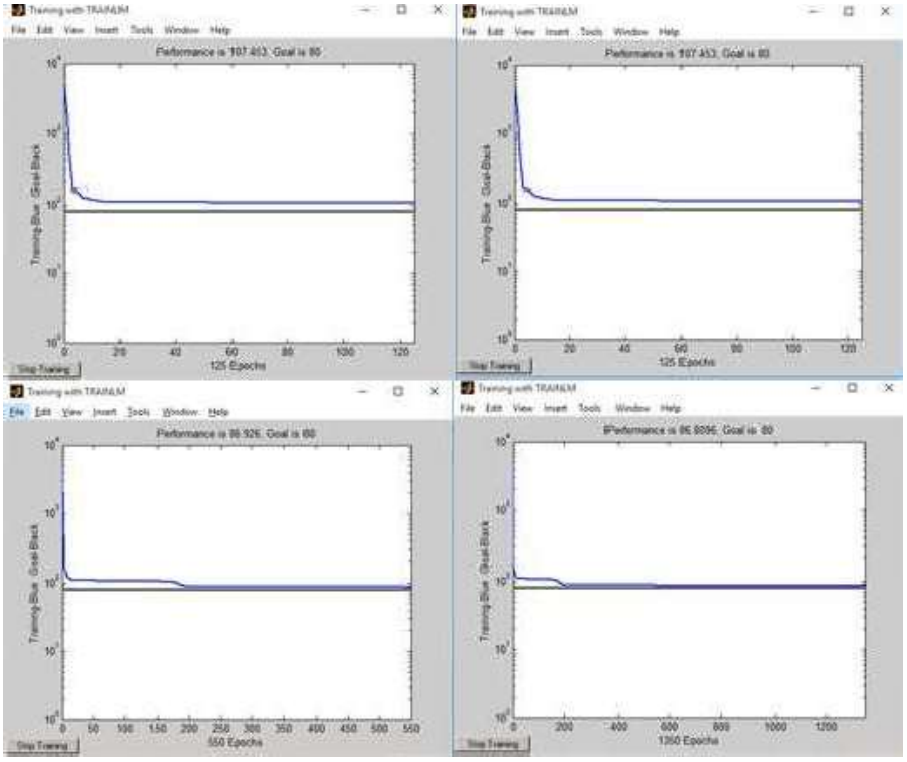
Setelah data-data sudah lengkap dan kriteria dari fungsi terpenuhi maka proses selanjutnya adalah melakukan uji simulasi pada jaringan yang telah dibuat sebelumnya, dengan cara menggunakan fungsi command " net=train(net,input,target) ", jika telah melakukan fungsi command ini maka akan muncul proses analisa dalam sebuah jaringan yang memperlihatkan kekuatan dari signal-signal gelombang jaringan tersebut. Berikut hasil output keluaran yang ditampilkan pada jaringan Neural Network :



Gambar 9. Proses Running Neural Network

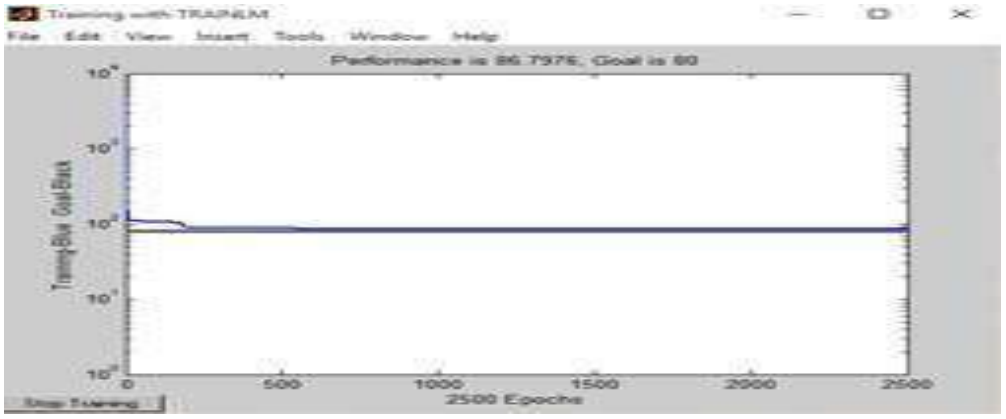
Proses ini memperlihatkan nilai-nilai tertentu yang didapat dari simulasi sebuah jaringan dengan mengikuti panjang data yang telah ditentukan. Berikut gambaran ouput tentang kekuatan jaringan dari mula proses hingga akhir sebuah proses jaringan.

p-ISSN: 1907-0012 e-ISSN : 2714-5417



Gambar 10. Output analisa jaringan Neural Network

Pada analisa sebuah jaringan ini dapat disimpulkan bahwa jaringan mengalami penurunan performance dari kondisi awal performance sebesar 107,453 menjadi 86,7976 dan kondisi ini diakibatkan karna terdapat sebuah permasalahan yang timbul dari jalannya paket sebuah jaringan. Berikut hasil akhir yang diperlihatkan dari proses analisa jaringan.



Gambar 11. Hasil akhir analisa jaringan Neural Network

Sehingga dapat dinyatakan bahwa performa dari sebuah jaringan mengalami penurunan di akibatkan serangan yang timbul pada jaringan tersebut.

5. KESIMPULAN DAN SARAN

Serangan Distributed denial-of-service (DDoS) sudah sejak tahun 1990. Semakin hari serangan Ddosd semakin banyak karena banyak nya hacker dan pengetahuan admin semakin meningkat tentang serangan data berupa serangan Ddos.

1. Keluaran output yang di sajikan pada Matlab ini mengenai performance dari suatu jaringan, dengan memiliki kekuatan performa sebesar 0.185395
2. performa dari sebuah jaringan dapat tergolong sangat rendah dari harapan, ini disebabkan terjadinya suatu kendala atau permasalahan yang timbul akibat performance yang secara signifikan menurun. Pada permasalahan ini, tahap selajutnya adalah mencoba test kebenaran atas serangan DDOS yang telah terjadi dengan bantuan aplikasi MatLab untuk menganalisa sebuah jaringan tersebut
3. Dibetuhkan pelatihan dan pengamanan yang kuat agar serangan Dods tidak mampu menyerang user.

DAFTAR PUSTAKA

[1] Arius, D. (2008). Computer Security (pp. 1–372). Yogyakarta: Andi OFFSET.

[2] Dharma, M. A. A. (2014). Keamanan Jaringan Komputer "DOS, DDOS & cara penaggulangannya" Disusun, (8053111064).

[3] Irsyad, M. M. (2015). Analysis System Anomaly Traffic Detection with Comparing The Diffrences of Triangle-Area-Map Features for Anomaly Type Identification Mujp. *Telkom University*, *2*(1), 254–263.

[4] Irsyad, M. M., Purwanto, Y., Purboyo, T. W., Prodi, S., & Komputer, T. (2015). Analysis System Anomaly Traffic Detection with Comparing The Diffrences of Triangle-Area-Map Features for Anomaly Type Identification. *Univ Telkom Journal*.

[5] Kato, K., & Klyuev, V. (2014). An Intelligent DDoS Attack Detection System Using Packet Analysis and Support Vector Machine. *International Journal of Intelligent Computing Research*, *5*(3), 464–471.

[6] Muhammad, A. W. (2016). Analisis Statistik Log Jaringan Untuk Deteksi Serangan Ddos Berbasis Neural Network. *Jurnal Ilmiah ILKOM*, *8*(Desember), 220–225. https://doi.org/10.13140/RG.2.2.19805.10723

[7] Muhammad, A. W., & Riadi, I. (2017). Deteksi Serangan DDoS Menggunakan Neural Network dengan Fungsi Fixed Moving Average Window, *1*(3), 115–122.

[8] Oo, T. T., & Phyu, T. (2013). A Statistical Approach to Classify and Identify DDoS Attacks using UCLA Dataset, *2*(5), 1766–1770.

[9Prasad, K. M., Reddy, A. R. M., & Rao, K. V. (2014). DoS and DDoS Attacks: Defense, Detection and TracebackMechanisms -A Survey, *14*(7).