Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 656-655 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Simulation Analysis Of Denial Of Services At The Computer Network

Muhammad Amin[1], Adli Abdillah Nababan[2]

[1]Sistem Komputer, FakultasSainsdanTeknologi
[2]Rekayasa Perangkat Lunak

[1]Universitas Pembangunan Panca Budi Medan,
[2]STMIK Pelita Nusantara
[1]Jl. JenderalGatotSubroto, KM 4,5SeiSikambing 20122 Medan, [2]Jl. IskandarMuda No.1, Medan

Email: [1]mhdamin9977@gmail.com, [2]adliabdillahnababan@gmail.com

ARTICLE INFO

Article history:
Received: 25/01/2020
Revised: 02/02/2020
Accepted: 06/02/2020

Keywords:
Systems, Denial of Services, Networks, Servers, Attacks

ABSTRACT

Denial of service is a type of attack whose purpose is to prevent real users from enjoying the services provided by the server. The server is a server that must always be ready to serve user requests, which generally operate 24 hours without stopping. There are several studies on denial of services (DOS) attacks, from research conducted there that examines denial of services (DOS) attacks on web security. Every attack carried out on the web application, every user accessing the web application will occur buffering data so that the user accessing the web application occurs obstacles and even lost data. General problems that occur in the DOS attack detection system (Denial of Services) is a way to prevent DOS attacks that are being carried out on an application or web system with a DOS attack detection system. The simulation of a DOS attack detection system (Denial of Services) made for this research as tool or media to find out DOS attacks that are happening on a local network. Simulation of a DOS (Denial Of Services) attack detection system is expected to be able to analyze every attack that occurs on the network locally and be able to analyze every attack that occurs on a local network simulation. In this research it is expected that the analysis carried out on a DOS attack detection system (Denial of Services) can be used as a reference as a detection of DOS attacks (Denial of Services) in general which is used to detect DOS attacks that occur in other applications

1. Introduction

During national holidays we often find it very difficult to send messages and make phone calls, even failing to send services often when calling is busy. This happened because there were so many people who texted during national holidays and called during quizzes that made the telecommunications network so busy that it could not serve other users.That event is similar to what happens when a server gets a Denial Of Service (DOS) attack.DOS is not the type of DOS that kills the server, but the type of DOS that busines the server.

Denial of Service (DOS) is a type of attack whose purpose is to prevent users from enjoying services provided by the server.Servers are servants who must always be ready to serve user requests, which generally operate 24 hours without stopping. An example is a web server that is in charge of serving web visitors providing information in the form of HTML pages.Under normal conditions, visitors can request resources from the web server to be displayed in their browser, but if the web server is hit by a DOS attack then the visitor cannot enjoy the web server service.

There are several motives for attackers in conducting Denial of Service, namely: to gain access, revenge, political reasons, and economic reasons. Therefore the writer will analyze the dos attack detection system on a computer network.

One of the exploits of denial of service (DOS) attacks is exploiting the weaknesses of web applications. Denial of Services (DOS) works by blocking the performance of a service or even turning off the service.This attack produces damage that is persistent meaning that the condition of denial of service will still occur even though the attacker has stopped attacking, and the server will return to normal after restarting / rebooting.

There are several studies about denial of services (DOS) attacks, from research conducted there that examines denial of services (DOS) attacks on web security. Every attack carried out on the web application, every user accessing the web application will occur buffering data so that the user accessing the web application occurs obstacles and even lost data.

.

2. Literature

A. System Aplication

"Aplication system is a collection of objects such as people, resources, concepts, and procedures that are intended to perform an identifiable function or to serve a purpose. For example, a university is a system of students, faculty, staff, administration, buildings, equipment, ideas, and rules with the aim of educating students, producing research, and providing services to communities (other systems)."[2].

B. Computer Netwoerk

"A computer network is a group of autonomous computers that are connected to one another through transmission media or communication media so that they can share data, information, programs, and use shared hardware such as printers, hard disks, and so forth.A computer network is a system consisting of collectionscomputers that are connected to each other that aims to shareinformation and information exchange communication resources.Every computer orPeripheral devices that are connected are called nodes, and computer networks areconnected with at least 2 computers on the network that have many nodes tens and even millions so that they are connected to one another, withintermediaries use copper cables, but some are with fiber optics,Bluetooth, even with satellite technology"[3].

C. Denial Of Services

Denial Of Servicesis a type of attack with the volume, intensity, and cost of mitigation that continues to increase as the scale of the organization grows.This study aims to develop a new approach to detect DDoS attacks, based on the characteristics of network activity using a neural network with a fixed moving average window (FMAW) function as a detection method. Training and testing data are taken from independent simulations.Denial of Service (DOS) is a type of attack whose purpose is to prevent real users from enjoying the services provided by the server.[4].

D. Website

Website or site can also beinterpreted as a collection of pages thatdisplay text data information, still or motion image data, animated data, sound,video and or a combination of these, all rightwhich is static or dynamic whichform a series of buildings whichinterrelated where each otherconnected to networkspage (hyperlink).Be static if the contents of informationWebsite fixed, rarely changed, and contentthe information is only in the direction of the ownerthe website. Are dynamic when contentswebsite information is always changing, andthe contents of the information are two-way interactivefrom website owners and users.[5].

3. Research Methods

A. Research Design

Broadly speaking, the stages of the entire study are as follows:

a) Describe the Problem

Describing the problem clearly will help in designing and making energy-efficient home lighting devices using solar panels using a microcontroller that will be studied must be described first, because without being able to describe the problem, determine and define the boundaries of the problem to be studied, then there will never be a solution the best of the problem. So this step is the most important first step in this research.

b) Problem Analysis
The problem analysis step is the step to understand the problem that has been determined in its scope or boundary. By analyzing the problems that have been determined, it is expected that the problem can be understood properly.

c) Setting Goals
Based on the understanding of the problems of the problem, the objectives to be achieved in this study are determined. In this goal the targets will be determined, especially those that can overcome the existing problems.

d) System Design
This stage is the design phase of the device made, at this stage the design of the device and the design of a series of local network equipment will be used as a test device.

e) Making The System
This stage is the stage for making simple local computer network devices based on the design and design of network devices that have been made in the previous stage.

f) System Testing
Tool testing is done by testing the simulation of a local network as a means of measuring the level of attack in the local network and can then be analyzed as a result of an attack that occurs on one computer.

g) Testing Results
At this stage the process of drawing conclusions and suggestions about what should be done during the study. Basic conclusions and suggestions which are the result of analysis and discussion.

B. Research Design

In this study a block diagram design of the system is made. The block diagram design can be seen in the picture below:

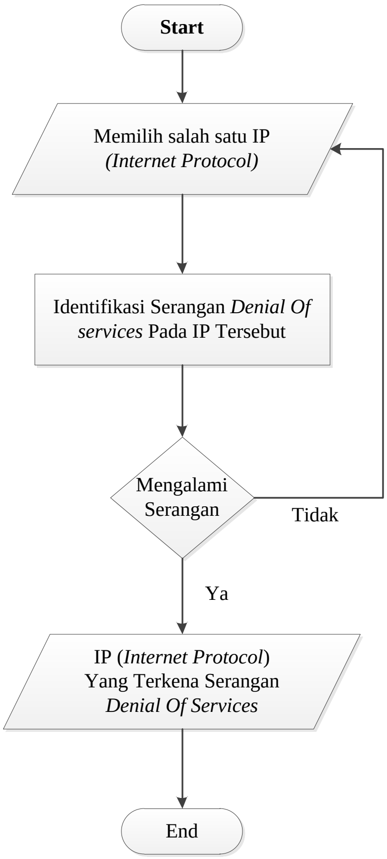
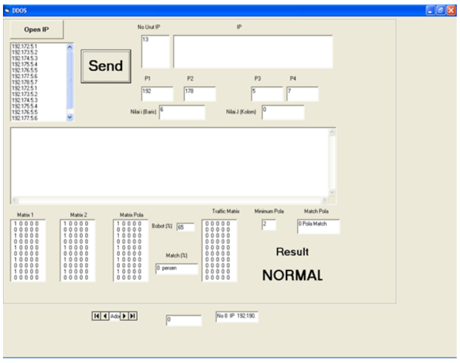

Start
Memilih salah satu IP
(Internet Protocol)
Identifikasi Serangan Denial Of services Pada IP Tersebut
Mengalami Serangan
Tidak
Ya
IP (Internet Protocol) Yang Terkena Serangan Denial Of Services
End

Fig 1. Circuit Block Diagram

In addition there is also the structure of the running of the program which is described in the form of flowchat. In Figure 1, it explains how the DOS (Denial of Services) attack detection system starts by selecting one of the ip (Internet Protocol) then sending the IP (Internet Protocol) process then the system will process the ip exposed to a denial of services attack or not, then will produce output if the ip is hit by a denial of services attack.

4. Results and Discussion

Before entering into the process of scanning IP (Internet Protocol), the author must obtain an IP (Internet Protocol) which is used to analyze denial of service attacks. IP (Internet Protocol) will be processed by a denial of services attack detection system and then the results of the process carried out by the denial of services attack detection system will be displayed. Denial of services attack detection system process can be seen in Figure 2 and Figure 3. The following is the process and results of the denial of services attack detection system from the computer under normal conditions.



192.172.5.1
192.173.5.2
192.174.5.3
192.175.5.4
192.176.5.5
192.177.5.6
192.178.5.7
192.172.5.1
192.173.5.2
192.174.5.3
192.175.5.4
192.176.5.5
192.177.5.6

No Urut IP: 13
IP:
P1: 192
P2: 178
P3: 5
P4: 7
Nilai i (Baris): 6
Nilai J (Kolom): 0

Matrix 1
```
1 0 0 0 0
0 0 0 0 0
1 0 0 0 0
0 0 0 0 0
1 0 0 0 0
0 0 0 0 0
1 0 0 0 0
0 0 0 0 0
1 0 0 0 0
0 0 0 0 0
```

Matrix 2
```
1 0 0 0 0
0 0 0 0 0
1 0 0 0 0
0 0 0 0 0
1 0 0 0 0
0 0 0 0 0
1 0 0 0 0
0 0 0 0 0
1 0 0 0 0
0 0 0 0 0
```

Matrix Pola
```
1 0 0 0 0
0 0 0 0 0
1 0 0 0 0
0 0 0 0 0
1 0 0 0 0
0 0 0 0 0
1 0 0 0 0
0 0 0 0 0
1 0 0 0 0
0 0 0 0 0
```

Bobot (%): 65
Match (%): 0 persen

Traffic Matrix
```
0 0 0 0 0
0 0 0 0 0
0 0 0 0 0
0 0 0 0 0
0 0 0 0 0
0 0 0 0 0
0 0 0 0 0
0 0 0 0 0
0 0 0 0 0
0 0 0 0 0
```

Minimum Pola: 2
Match Pola: 0 Pola Match

NORMAL

Ado
0
No 8 IP 192.190.

Fig 2. DOS Attack Detection System in a Normal State

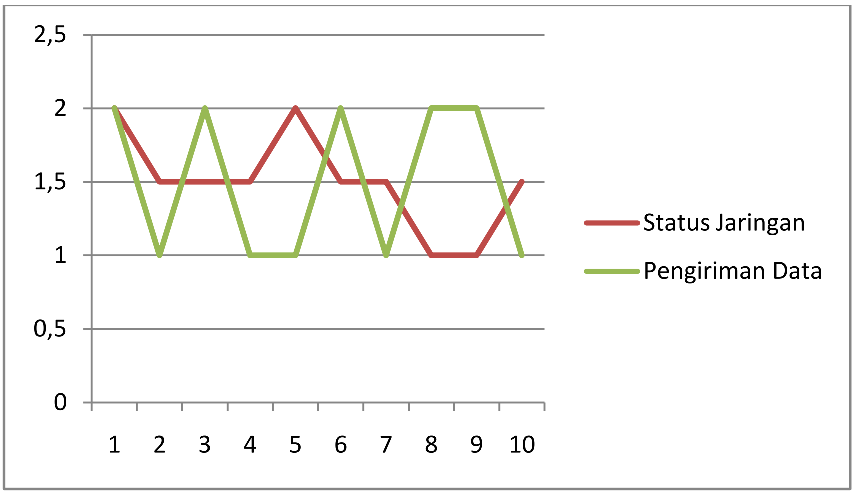


Fig 3. Network Condition Graph In Normal Condition

After analyzing the simulation of a denial of services attack detection system using Visual Basic 6.0 application like Figure 2 above, it is clear that the filtered IP (Internet Protocol) is the IP that makes a normal request, meaning that there is no IP that repeatedly sends data package or doing a DOS attack on a computer. This can be seen clearly when compared with Figure 4. The graph for a computer in a normal state does not experience attacks can be seen in Figure 3.

5. Conclusion

From the results and discussion of the research that has been done it can be concluded several things:

a) DOS attacks are attacks that occur within a computer network by flooding the network with many requests so that it consumes resources.
b) DOS attacks can be detected by Anomaly and Signature Based.
c) Computers affected by DOS attacks will experience increased traffic, a network that suddenly slows down, and an increasing amount of spam.
d) The purpose of DOS attacks is to prevent the client from gaining access from the server..

6. References

[1] Tasnuva Mahjabin, Yang Xiao, Guang Sun and Wangdong Jiang. “A Survey Of Distributed denial of service attack, preventation and mitigation technicques” Internasional Journal of Distributed Sensor Network Vol. 13 2017.

[2] Indra Riyana; Rita Puspitasari, "Local area network (lan) network analysis," 2018PROSISKO Jurnal Vol. 5 No. 1 Maret 2018.

[3] Arif Wirawan; Imam Riadi; Sunardi, "Detection of DDoS Attacks Using Neural Network with Fixed Moving Average Window Function", Sunan Kali Jaga Journal, 2018

[4] T Gunasekhar, K Thirupati, P Saikiran and P.V.S LAkhsmi. "A Survey On Denial Of Service Attack," Internasional Journal of Computer Science and Information TechnologiesVol. 5 2014

[5] Amin, M., Tulus., Ramli M . (2016). Modeling of robot balancing control using fuzzy logic withkalman filter: Teknovasi Journal Vol. 03 Nomor. 1 2016.