Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 41-49 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Security Of Dynamic Domain Name System Servers Against DDOS Attacks Using IPTABLE And FAIL2BA

Ibnu Muakhori[1], Sunardi[2], Abdul Fadlil[3]

[1,2,3]Magister Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta

Email: ibnu0176@gmail.com[1],sunardi@mti.uad.ac.id[2],fadlil@mti.uad.ac.id[3]

ARTICLE INFO

Article history:
Received: 12/02/2020
Revised: 09/03/2020
Accepted: 01/05/2020

Keywords:
Security,
DDNS,
DDoS,
Fail2ban

ABSTRACT

Availability, integrity and confidentiality are the main objectives of information security and server security. These three elements are links that are interconnected in the concept of information protection.Distributed Denial of Service (DDoS) is an attack to make online services, networks and applications not available by flooding data traffic so that services is unvailable or availability aspects disrupted. This attack resulted in huge losses for institutions and companies engaged in online services and web-based applications being one of the main targets of attackers to carry out DDoS attacks. Countermeasures that take a long time and large recovery costs are a loss for the institution or company that owns the service due to loss of integrity. NDLC (Network Development Life Cycle) is a method that has stages namely analysis, design, simulation, prototyping, implementation, monitoring and management. The NDLC method used aim for the results obtained focused and detailed. Snort IDS applied on the DDNS server functions to record when there is a DDoS attack. Implemention fail2ban as realtime preventation tool on the server by configuring based on the rules applied to fail2ban. The results showed Snort IDS managed to detect DDoS attacks based on the rules applied to Snort IDS. Realtime prevention using Fail2ban successfully functions as a DDoS attack by blocking the attacker's IP Address.

1. Introduction

Server security is a top priority for network administrators. Along with the rapid development of the internet world and internet users more and more so that the information stored on the server is very important to maintain. On the other hand the many security threats in computer network systems make network administrators need to anticipate this, especially DDoS attacks. DDoS attacks are attacks that are difficult to overcome. There are several ways to carry out DoS attacks such as shutting down the server so that it keeps the server busy and sends many requests [1]. So that on computer security, objects that need to be protected are computers and information [2].

Fail2ban is a program package to detect failed login attempts and then block the IP address of the original host [Fail2ban.org], Fail2ban works by changing the firewall configuration rules (IPTable) with configurations that are in Fail2ban itself, when Fail2ban runs, it will retrieve over the firewall functions that are on the server [3]. Using Fail2ban "on an Ubuntu server is proven to prevent bruteforce attacks and block the ip address of the attacker [7,9]. Fail2ban can secure various servers and then provide the results of attacks in the form of log data. Based on the above problems, a network administrator needs a system that can provide assistance in preventing DDoS attacks in real time. A system that can help administrators if they are not in place conditions. Through this research, it is expected to facilitate the network administrator in carrying out its functions properly. IPTable and Fail2ban are able to answer the above problems well.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 41-49 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

2. Research Methods

In this study the research method adopted was using the Network Development Life Cycle (NDLC) method. NDLC is a method that relies on previous development processes such as business strategy planning, application development life cycle, and data distribution analysis [4]. The stages of the NDLC method can be explained as follows (Figure 1):

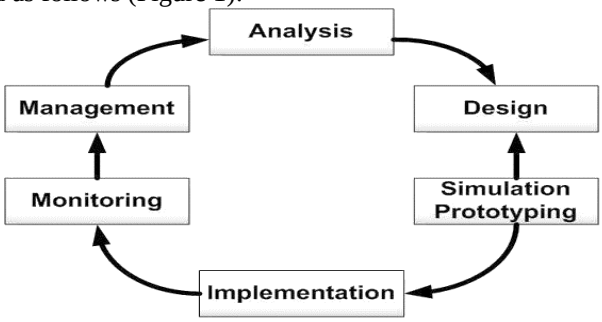

Fig 1 : NDLC

3. Result

a. Research Stages

Stages of research are used as guidelines in conducting research so that the results achieved do not deviate from the goal. Figure 2 shows the flowchart of the stages of the research to be carried out. The stages begin with Analysis, Design, Simulation Prototyping, Implementation, Monitoring and management.

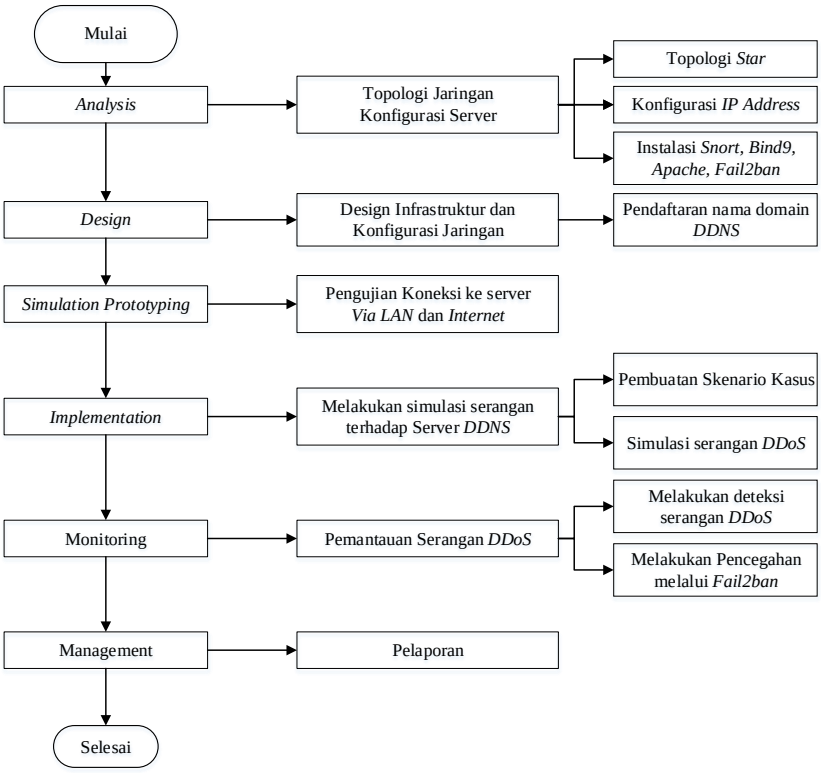

Fig 2. Flowchart Research Stages

b. Testing Scenario

The testing scenario uses 2 tools, LOIC and Dark Fantasy, with 2 scenarios, namely:

1. Scenario of Attack Through Local Network (LAN)

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 41-49 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

2. Scenario of Attack Through the Internet Network

c. Network Design

Network design uses star topology which can be seen in Figure 3.

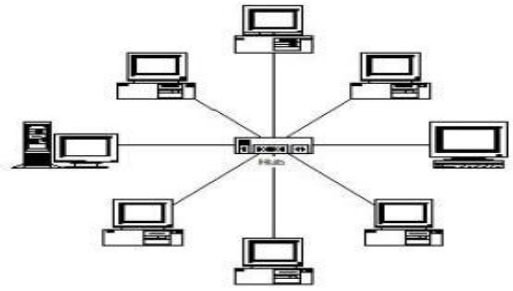

Fig 3. Topology Star[8]

The choice of star topology is because the topology uses a switch or hub as a network connection media and is not dependent on other computers.

Based on the star topology, researchers conducted a network design as illustrated in Figure 4

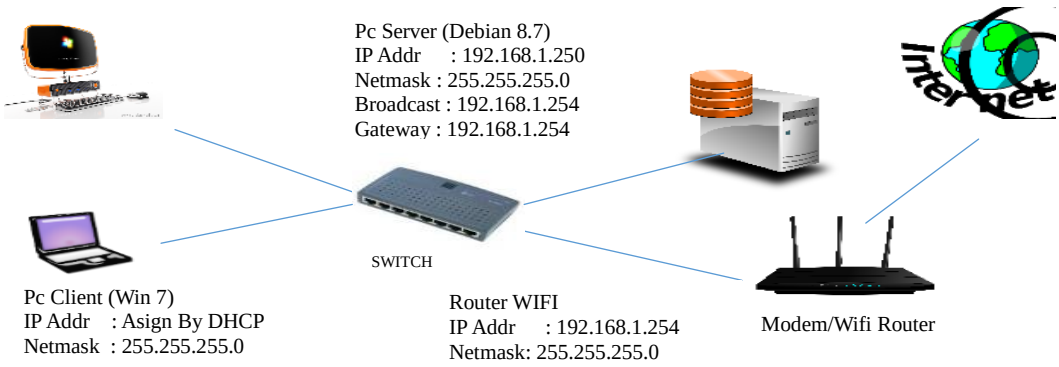

Fig 4. Network Design

d. Installation, configuration of IPTable and fail2ban

Configure DDoS on fail2ban with the command sudo nano /etc/fail2ban/jail.local

```
# DDoS
[http-get-dos]
#enabled = true
port = http,https
filter = http-get-dos
#Path to your logs
#To add all logs in a folder add Wildcard (*) expression
logpath = /var/log/fail2ban/*_access_log
#Max number of requests
#maxretry = 500
#Findtime in seconds
#findtime = 120
#Bantime in seconds - set negative to ban forever
bantime = -1
#Action - change sendmail to send to your email
action = iptables[name=HTTP, port=http, protocol=tcp]
```


Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 41-49 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

d. Case Scenario

Before the test was carried out, researchers recorded the IP address of the attacker's computer. This is intended to make it easier to identify (Table 1 and Table 2).

Table 1
IP Address lokal (LAN) Attacker

No	IP Address Attack	Tools	Port Attack
1	192.168.1.10	cmd	80
2	192.168.1.11	Darkfantasy	80
3	192.168.1.12	Loic	22
4	192.168.1.13	Loic	53

Table 2.
IP Address Internet Attacker

No	IP Address Attack	Tools	Port Attack
1	104.237.144.6	Cmd	80
2	180.240.190.184	Darkfantasy	80
3	125.160.139.182	Loic	22
4	125.160.139.182	Loic	53

Table 1 and Table 2 show that there are four local IP addresses (LANs) and Internet IP Addresses, each of which is identified as the attacker's IP address and uses predetermined tools.

e. DDOS Attack Simulation

Based on the case scenario, the next process is testing the DoS attack from the Host which acts as an attacker to the DDNS server as set forth in Table 3.

Table 3
Simulation Attacker DDoS

No	Pengujian	Tools yang digunakan	Port Target
1	Attempted DDoS attack via local network and internet	Command Prompt : Ping tamelin.ddns.net –l 5000 –n 5000 –w 1	80
2		DarkFantasy	80
3		Loic	53 dan 22

Table 3 is an attack step that will be carried out in testing both in the local network (LAN) and through the internet network. In testing it is expected that fail2ban is able to block the attacker's IP Address. The attack simulation can be explained as follows:

1) Ping of Death Attacks

Attackers do DoS attacks using the Windows command prompt for 30 minutes (Figure 5). The command that is run by the attacking computer is:

```
Ping tamelin.ddns.net –l 5000 –n 5000 –w 1
```

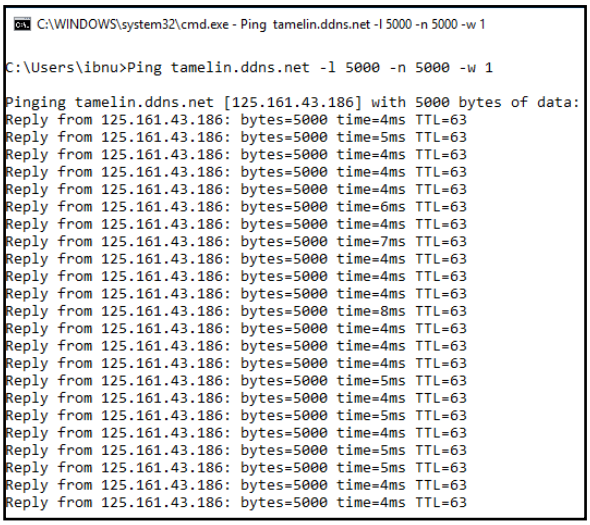

Fig 5. DDoS attacks use Command Prompt

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 41-49 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

2) Attack using Darkfantasy

Attack simulation using darkfantasy with the following steps (Figure 6):

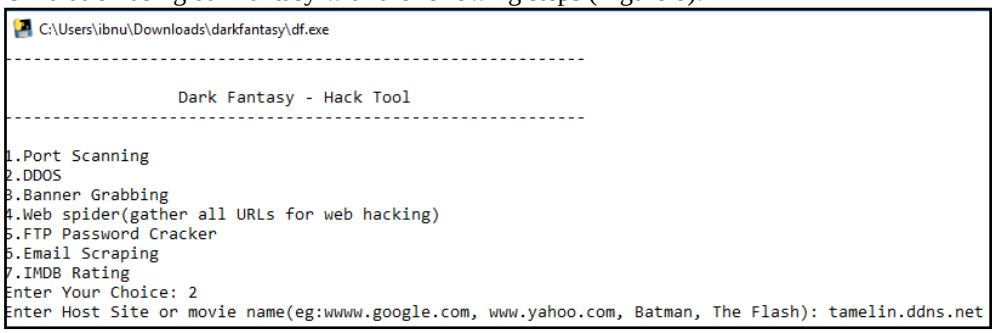

Fig6. Start a DDoS attack using Darkfantasy

The parameters used by Darkfantasy are as follows:
Target site: tamelin.ddns.net
Number of Packets to be sent: 1,000,000
The process of synflooding in dark fantasy can be seen in Figure 7

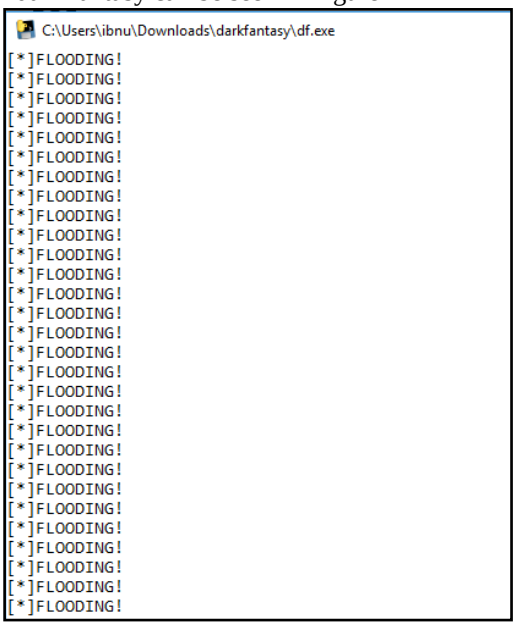

Fig 7. SynFlooding Darkfantasy

3) Attacks using LOIC software

Attack simulation using LOIC with the following parameters (Figure 8):
url: the target url is tamelin.ddns.net
IP: LOIC will automatically get an IP Address
Method: TCP
Ports: 53 and 22
Threads: 50 (Number of threads used to attack)
Time out: 9001 (time range of package delivery)

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 41-49 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

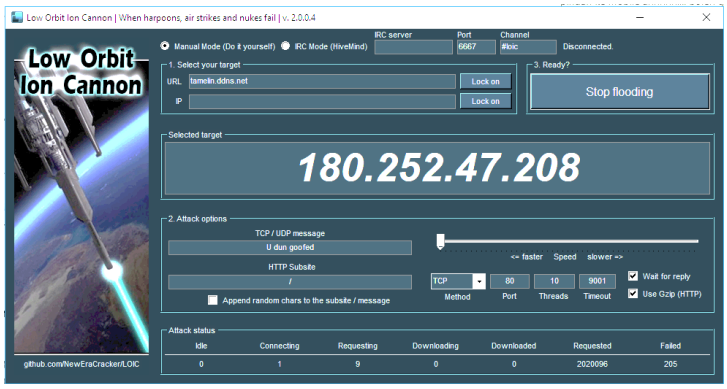

Fig 8. DoS attacks with LOIC

With parameters input to LOIC, it can be seen that the number of connections within 9001 ms, there are 30 connections, and 20 packet requests sent to the server. If the number of failed appearances exceeds the number of requests it can be ensured that the DDNS server has experienced an error.

f. Testing Results

Fail2ban which is used to carry out prevention against DDoS attacks is by blocking IPAddress the attacker has successfully performed its function properly. It can be seen in Figure 9 that the total release block is 102,160 requests. It can be concluded that the blocking process carried out by fail2ban in realtime runs perfectly. The number of packets analyzed by fail2ban is 46 packets (92%) with the breakdown of packets via the IP address protocol V4 of 46, TCP as much as 31, UDP of 15 packets.

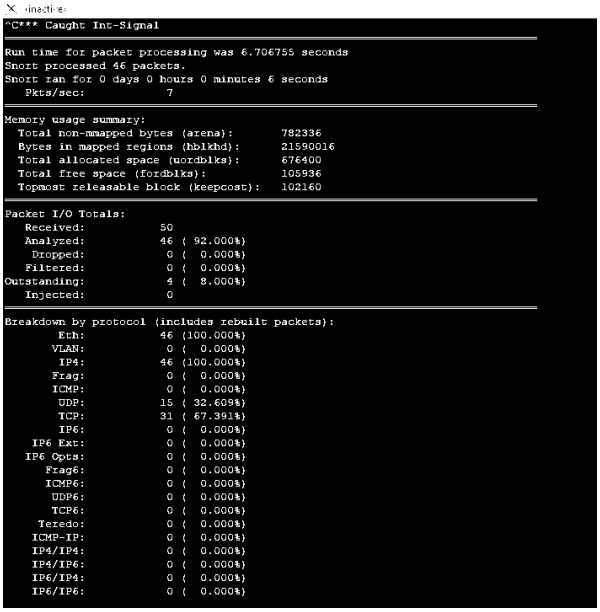

Fig 9. Fail2ban Log

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 41-49 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

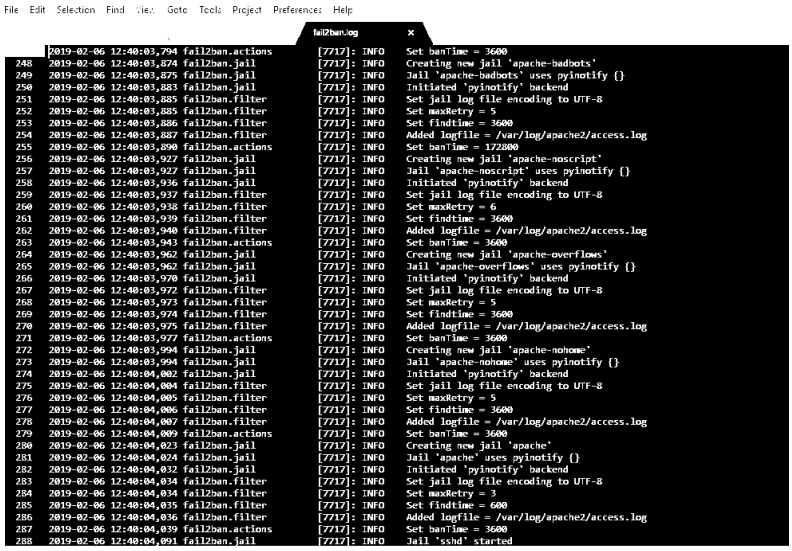

Fig 10. Fail2ban.log

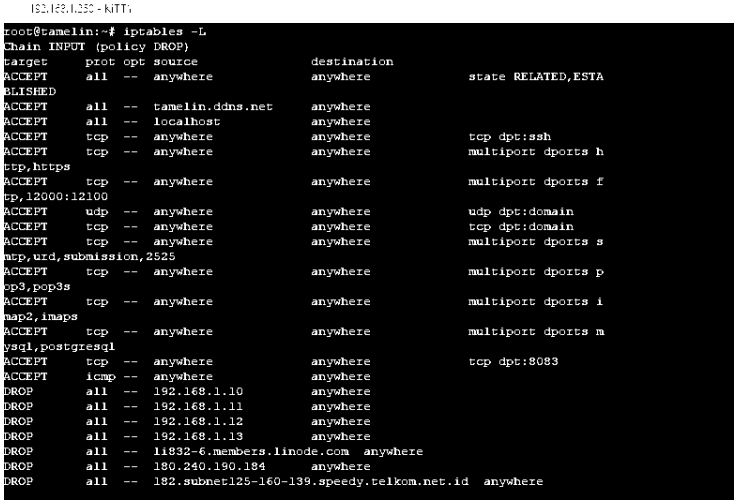

Fig 11. Fail2ban.log

Fail2ban saves the detection results in the form of a Log file. Through the Log File it can be seen that there are indications of an attack which causes interference with the DDNS server (Figure 10) and successfully blocks the attacker's IP Address (Figure 11)

Table 4
Blocked Local IP Address Attacker

No	**IP Address** Attacker	**Tools**	**Port** Attacker	**Blokir**
1	192.168.1.10	Cmd	80	✓
2	192.168.1.11	Darkfantasy	80	✓
3	192.168.1.12	Loic	22	✓
4	192.168.1.13	Loic	53	✓

Table 5
Blocked Internet IP Address Attacker

No	**IP Address** Attacker	**Tools**	**Port** Attacker	**Blokir**
1	116.66.249.102	Cmd	80	✓
2	180.240.190.184	Darkfantasy	80	✓
3	125.160.139.182	Loic	22	✓
4	36.84.144.20	Loic	53	✓

After blocking the walk, the attack simulation was again carried out using Darkfantasy and Loic.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 41-49 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Darkfantasy displays the Unable to connect message (Figure 12), while Loic does not produce the amount of connecting (Figure 13), this indicates that the attacker's IP Address that has been blocked by fail2ban cannot re-attack. In addition to these two tools, access rights through the browser application can no longer be opened by the attacker (Figure 14).

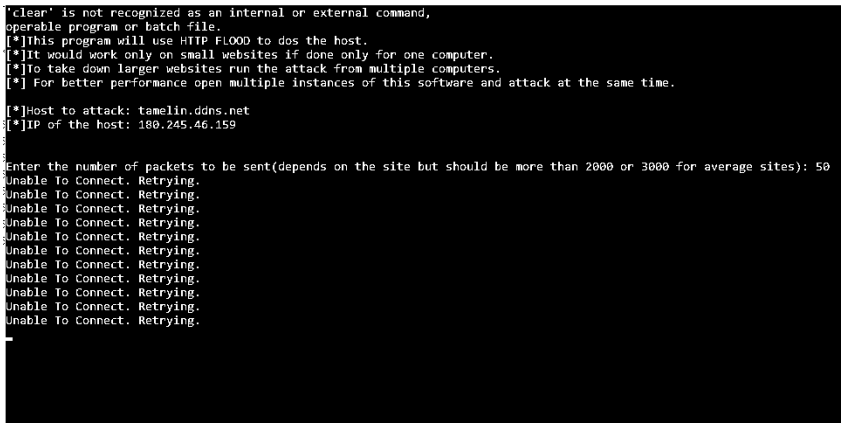

Fig 12. Darkfantasy after the IP Addr attacker is blocked.

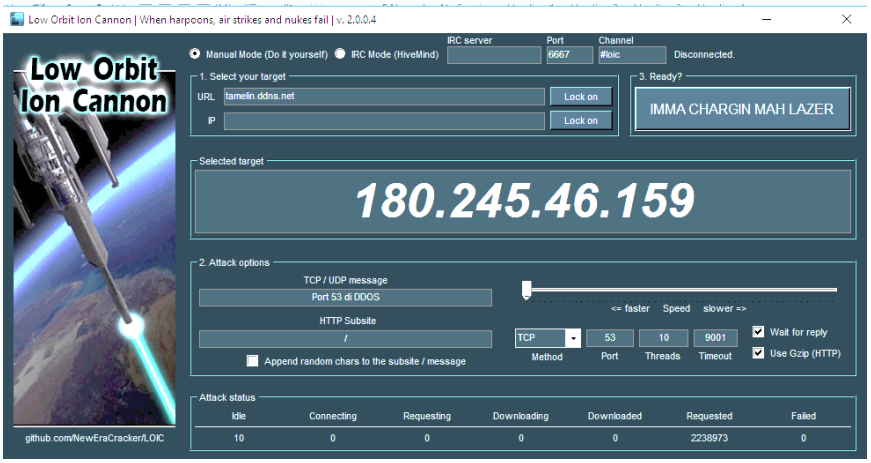

Fig 13. Display LOIC after the attacker's IP Address is blocked

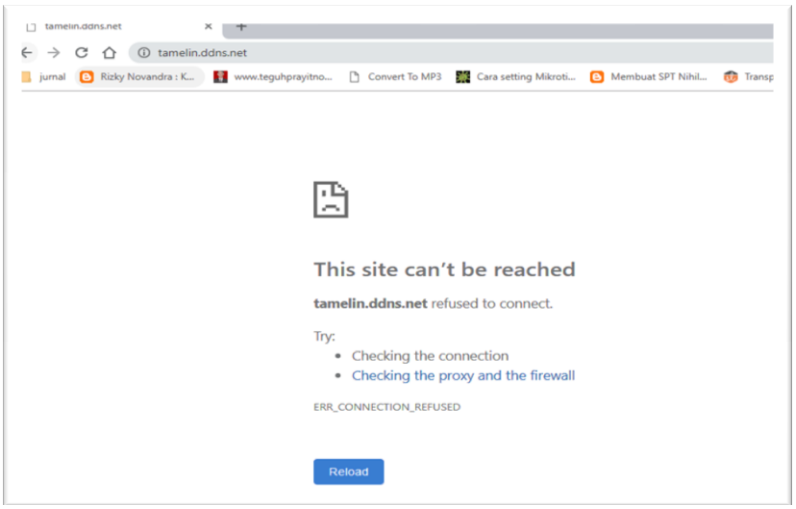

Fig 14. Browser application from the attacker

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 41-49 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

4. Conclusion

The conclusion that can be drawn from this study is that IPTable and Fail2ban can prevent DDoS attacks by blocking the IP Address of the attacker. The next research is to make security on the types of Bruteforce attacks and security of web server and email server services. It is expected that IPTable and Fail2ban can prevent Bruteforce attacks and secure the service. So that network administrator performance becomes easier.

5. References

[1] Purba, Riverta Fierre Dwiputra. (2018), Simulasi Pencegahan Serangan Denial Of Service (DoS) Pada Software-Defined Networking (SDN) Menggunakan Intrusion Prevention System (IPS) dan Algoritma Genetika, Universitas Sumatera Utara.
[2] K. J.M, "Guide To Computer Security Third Edition," Chattanooga: Springer, 2014.
[3] Suroto, John Friadi, "Membangun Sistem Keamanan Komputer Untuk Menghadapi Serangan Bruteforce dengan menggunakan Fail2Ban", Seminar Nasional Teknologi Informasi dan Komunikasi Terapan (SEMANTEK), 2015
[4] Iwan Kurniawan, Ferry Mulyanto, Fuad Nandiasa, "Sistem Pencegahan Serangan Bruteforce Pada Ubuntu Server Dengan Menggunakan Fail2ban",Vol 18 No 2, Infomatek Universitas Pasundan, 2016
[5] Hendra Kurniawan, Sandy Kosasi. (2015), Penerapan Network Development Life Cycle Dalam Perancangan Intranet Untuk Mendukung Proses Pembelajaran, Jurnal Ilmiah Sisfotenika Vol. 5, No. 2 Juli 2015.
[4] Ibnu Muakhori, "Membangun Webserver Menggunakan Dynamic Domain Name System (DDNS) Berbasis Berkeley Internet Name Domain (BIND 9) Pada IP Dinamis"Jurnal Sistem Informasi (JSI) Universitas Dirgantara Marsekal Suryadarma, 2018
[6] Mokhomad Aguk Nur Anggraini, " Uji Fitur Intrusion Prevention Pada Firewall Untangle dengan Pengujian DOS dan ,SSH Bruteforce", Volume 9 No 01, Jurnal Manajemen Informatika Universitas Negeri Surabaya 2018
[7] Syaifuddin, Diah Risqiwati, Eko Ari Irawan. (2018), Realtime Pencegahan Serangan BruteForce dan DDOS Pada Ubuntu Server, Techno.COM, Vol. 17, No. 4, November 2018, 347-354.
[8] Ritzkal, Manajemen Jaringan Untuk Pemula,Bogor:UIKA PRESS,2018
[9] Ritzkal, Keamanan Jaringan Cyber,,Bogor:UIKA PRESS,2019

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.