e-ISSN: 2614-8404
p-ISSN:2776-3234

DDoS ATTACK MITIGATION WITH INTRUSION DETECTION SYSTEM (IDS) USING TELEGRAM BOTS

Mohammad Taufan Asri Zaen[1*)], Ahmad Tantoni[2], Maulana Ashari[3]
[1,3]Program Studi Studi Sistem Informasi, STMIK Lombok
[2]Program Studi Teknik Informatika, STMIK Lombok
Email: [1]opanzain@gmail.com, [2]ahmad.tantoni@students.amikom.ac.id, [3]aarydarkmaul@gmail.com

Abstract – In the current IS/IT era, service to consumers is an absolute must to be prepared to survive in business competition. Physical and logical attacks with the aim of disrupting information technology services for individuals/agencies/companies or reducing the performance of IS/IT used. The development of IoT in the industrial revolution 4.0, which is all online, is a challenge in itself, from a negative point of view, all of them are able to carry out attacks on ISP servers, often carried out by hackers. DDoS (Distributed Denial of Service) attacks are the most common attacks. The development of software for DDoS attacks is very much on the internet, including UDP Unicorn software to attack very easily and can be done by anyone. Software for real-time monitoring of DDoS attacks, one of which is the Telegram bot. Telegram is a messaging system centered on security and confidentiality, while bots are computer programs that do certain jobs automatically. Telegram bot is free, lightweight and multiplatform. In the case study, this research contains 10 access points to the internet that will be mitigated from DDoS attacks. In this study, it was found that DDoS attacks caused traffic to become very high/congested by fulfilling upload traffic so that legitimate traffic users could not access the internet, connection to the internet was slow, the traffic was also unnatural, making it unable to connect to wireless devices and making Mikrotik loginpage becomes unable to appear. The purpose of this study is to mitigate DDoS attacks with the help of telegram bots so as to facilitate the notification of DDoS attacks in the event of an attack so that it is fast to deal with and find the perpetrators of the attack. The conclusion of this study is that DDoS attacks using UDP unicorn software resulted in a traffic spike of 53.5 Mbps on the upload traffic side, causing traffic for legitimate/authenticated users to slow down. By using telegram bots to know DDoS attacks occur in real time with a success rate of attack detection up to 100% notifications on telegram bots. Mitigation of DDoS attacks takes steps to track users using the torch feature on the routerboard interface menu, trace internet connection lines using wired or wireless transmission media, and ensure always monitoring the proxy interface from winbox.

Keywords – Attack Mitigation, DDoS, IDS, Telegram

I. INTRODUCTION

The need for network security is very important in the world of information technology and information systems. In the current IS/IT era, service to consumers is an absolute must to be prepared to survive in business competition. There are times when irresponsible people make attacks on information technology systems and networks that are developed. The attack is in the form of physical and logical attacks with the aim of disrupting information technology services for individuals/agencies/companies or reducing the performance of information systems and information technology used.

The development of IoT (Internet of Things) in the industrial revolution 4.0 which is all online is a challenge in itself, everyone can access anything from the virtual world, from the negative side, everyone is able to attack a service on the internet. Several attacks on servers as internet service providers (ISPs) are often carried out by hackers with various purposes. DDOS (Distributed Denial of Service) attack is an attack that may often be found among other attacks.

The development of software to carry out DDoS attacks is also very widely spread on the internet, including UDP Unicorn software, which is a software that uses a very easy way to attack and can be done by anyone, and there are many more software to carry out DDoS attacks on the internet.

In monitoring computer networks when a DDoS attack occurs, there are many applications that can be used to monitor DDoS attacks in real time, one of which is the telegram bot. Telegram is a cross-platform messaging system centered on security and privacy, while bots are computer programs that do certain jobs automatically.

Telegram bot is a bot that is currently popularly used among the public because it is free, lightweight and multiplatform. Telegram also has a fairly complete and growing Bot API. The famous telegram bot is the telegram-bot made by Yago Perez [1].

In the case study, this research contains 10 access points to the internet that will be mitigated from DDoS attacks. In this study, it was found that DDoS attacks caused traffic to become very high/congested by fulfilling upload traffic so that legitimate traffic users could not access the internet, connection to the internet was slow, the traffic was also unnatural, making it unable to connect to wireless devices and making Mikrotik loginpage becomes unable to appear.

The problem of this research how to mitigate DDoS attacks carried out by using a bot Unicorn UDP telegram. The purpose of this study is to mitigate DDoS attacks with the help of telegram bots so as to facilitate the notification of DDoS attacks in the event of an attack so that it is fast to deal with and find the perpetrators of the attack.

Research conducted by Nadila Sugianti et al with the title Detection of HTTP-Based Distributed Denial of Services (DDOS) Attacks Using the Fuzzy Sugeno Method. The purpose of this research is to create an application to detect HTTP-based DDOS attacks with good accuracy using the fuzzy Sugeno method. Based on the discussion that has been explained and the results of tests that have been carried out, HTTP-based DDOS attack detectors based on the number of users, the number of packets, the number of packets/users and the length of the data captured by fuzzy logic using the Sugeno method can be used as a detector in determining DDOS attacks based on HTTP with an accuracy rate of up to 90% [2].

Research conducted by Jodi Chris Jordan Sihombing et al with the title Implementation of Distributed Denial of Service (DDoS) Attack Detection and Mitigation System using SVM Classifier on Software Defined Network (SDN) Architecture. The research objective is to implement a system that can detect and mitigate DDoS attacks on the SDN architecture. Conclusions from the research 1) The DDoS attack detection and mitigation (SDMD) system using the SVM classifier can be applied to the SDN architecture. 2) The DDoS attack mitigation mechanism is carried out by adding a flow rule on the switch to filter packets that go to the victim host. After the flow rule is added to the switch's flow table, the switch will drop every packet originating from the attacker's source IP, but any packets originating from the legitimate host's source IP will be forwarded. 3) SDMD performance in detecting DDoS attacks is very good. The accuracy obtained in detecting DDoS attacks is 96.08%, 95.66%, and 98.76% for syn flooding, udp flooding, and icmp flooding, respectively [3].

Research conducted by Muhammad Aziz et al with the title Implementing Artificial Neural Networks to Detect DDoS Attacks in Network Forensics. The purpose of the study is to determine the accuracy of DDoS attacks for network forensic purposes, the proposed method to analyze and test DDoS attacks detected on IDS with datasets at the Research Laboratory of Masters in Informatics Engineering, Ahmad Dahlan University (LRis-MTIUAD) using artificial neural network (ANN) methods based on calculations statistics. The conclusion from the research is that the attack information that has been detected by signature-based IDS needs to be reviewed for accuracy using classification with statistical calculations. Based on the analysis and testing carried out by the artificial neural network method, it was found that the accuracy was 95.2381%. Artificial neural network methods can be applied in the field of network forensics in determining accurate results and helping strengthen evidence at trial [4].

Research conducted by Eddy Prasetyo Nugroho et al with the title Security Reporting System on Cloud Computing Networks Through Telegram bots using Intrusion Detection and Prevention System Techniques. The conclusion of the research is to build an intrusion detection system by producing output not only in the form of records of intrusion activities on the database but also notifications via instant messaging Telegram. The results of recording intrusion activities in the database are used as data to perform network forensic analysis regarding the identity of the source of incoming packets, as well as to analyze the level of IDS system responsibility both in detecting attacks and sending notifications to administrators [5].

The research conducted by Jefree Fahana et al with the title Using Telegram as an Attack Notification for Network Forensics Purposes. The purpose of the research is to help network administrators to make it easier to find attacks that are usually carried out manually. The conclusion of the study was that it was successful in detecting attacks by using Snort. Alerts work very well and are able to send information to the database which is then forwarded using the telegram instant messenger application in real time. The results show that there has been a ddos attack via ICMP based on the log analysis performed [6].

1.1 Intrusion Detection System (IDS)

Intrusion Detection System is a prevention system using software or hardware that works automatically to monitor the situation on a computer network and can analyze network security problems. IDS is a tool, method and resource that provides assistance in identifying, reporting on computer network activity [7].

The ability of the IDS is to provide an early warning to the Network Administrator when a certain activity occurs that the Administrator does not want. In addition to providing warnings, IDS is also able to track activities that harm a system. An IDS can monitor packets passing through the network and try to find out if there is any suspicious activity.

IDS functions to monitor unusual activities on the network so that the initial steps of the attackers can be known. Thus the Administrator can take precautions and be prepared for what might happen.

In recognizing attack patterns, there are several methods of how IDS works, namely: Signature Based IDS and Anomaly Based IDS.

a) Signature Based IDS

A signature-based IDS will monitor the packets in the network and compare these packets with the signature database owned by this IDS system. This method is almost the same as how antivirus applications work in detecting malware. The point is that there will be a delay between the detection of an attack on the internet and the signature used for detection which is implemented in the IDS database used. So it could be that the signature database used in the IDS system is not able to detect an attempted attack on the network because the information on this type of attack is not contained in the signature database of this IDS system. During this time delay, the IDS system cannot detect any new types of attacks.

b) Anomaly Based IDS

This type will monitor the traffic in the network and compare the traffic that occurs with the average traffic (stable). The system will identify what is meant by a "normal" network in the network, how much bandwidth is usually used on the network, what protocols are used, what ports are usually interconnected with each other in the network and alert the administrator. when detected something is not normal.

The anomaly-based IDS method offers advantages over the signature-based IDS, which is that it can detect new forms of attacks that are not yet included in the IDS signature database. The downside is that this type often emits false positive messages. So that the Administrator's task becomes more complicated, by having to sort out which is the real attack from the many false positives that appear.

1.2 Distributed Denial of Service

According to Mousavi (2014), Distributed Denial of Service attack (DDoS) is an attack carried out on all the bloat or computer network by sending the dense traffic [8]. DDoS attacks start from attackers who distribute attacks using machines. During an attack, all traffic is directed to the victim's computer or server to consume the victim's resources. DDoS attacks will often use IP spoofing with the aim of flooding the target with high traffic while masking the identity of the original source to prevent mitigation efforts. If the source IP address is spoofed and continues to be scrambled, attempts to block attacks will become difficult. According to Kumarasamy (2012), there are several types of DDoS attacks [9] including the following :

1. TCP SYN Flooding: Is a type of attack that exploits the 3 way handshake mechanism in the TCP protocol, the attacker sends a large number of SYN packets to overload the target being attacked.
2. UDP Flooding: Is a type of attack that exploits the UDP protocol, the attacker has a list of broadcast addresses to send fake UDP packets to. This packet delivery mechanism is sent to a random port and then changes the target location unexpectedly.
3. Ping (ICMP) Flooding: Is a type of attack against the ICMP protocol with the aim of depleting the victim's computer resources by flooding it through requests from ICMP echo or also known as the ping command.

1.3 Firewall Mikrotik

A firewall is a hardware device or software system or group of systems (routers, proxies, gateways) designed to allow or deny network transmissions based on a set of security rules and regulations to enforce control between two networks to protect the "inside" network from the "outside" network. Firewall acts as a filter between internal and external computers. The firewall performs control based on the source IP address, source and destination TCP/UDP ports, destination IP address, and header information stored in data packets [10].

1.4 Traffic Monitoring Mikrotik

Traffic Monitor is a feature in Mikrotik that is rarely used. This traffic monitor can be used to monitor traffic running on an interface on the router and can determine a traffic threshold value. If the traffic has reached the specified threshold, then Traffic Monitor can execute a script. Thus can use this feature for various needs by determining what scripts will be executed. Steps to activate Traffic Monitor in the required interface with the steps on the Tools menu → Traffic Monitor [11].

1.5 Telegram

The main attraction of Telegram is that it can run on various devices and operating systems, not only mobile phones, but also computers, smartphones and others. Telegrams and bots can make everyday life easier without having to just stare at the computer. At the beginning of the development of the bot world on Telegram, almost all bots were created using telegram-cli and lua. The telegram-cli bot works like a personal account, it can even log in as a telegram-cli bot account and do what normal accounts can do. The benefits of this bot were also acknowledged by Telegram, which then launched a bot API so that many people could build bots using the programming language they mastered without having to deal with Telegram-cli or MTProto. Bot API is a bot account, there are certain things that normal accounts can do that bot accounts can't, for example creating groups, adding people to groups and removing people from groups [12].

II. Research Methodology

2.1 Research Flow

The flow of this research is as follows :

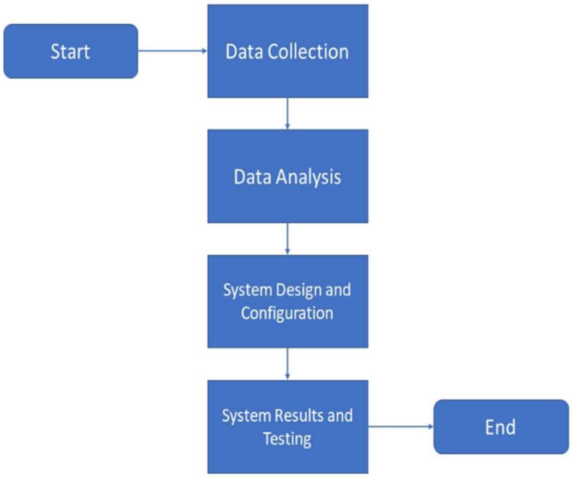


Figure 1. Research Flow

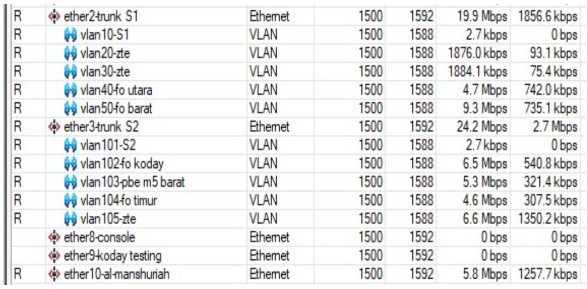
Figure 1. Shows the flow of the research carried out. The first step is data collection, which collects data on the form and DDoS attacks that are carried out. The second step is data analysis which performs analysis and techniques to prevent DDoS attacks. the third step is the design and configuration of the system which designs and implements DDoS attack mitigation techniques with telegram bots as notifications in the event of an ongoing attack. The fourth step is the results and system testing which is doing testing to find out whether the DDoS attack mitigation system runs smoothly as expected.

2.2 Data collection

Data collection with the tested parameters is to determine the target IP address, determine the packet size to be sent (flood), the path that is passed (threads), the socket path that is passed (sockets per thread) and the test time for 10 seconds ago. UDP unicorn software is run, then monitoring is carried out from the mikrotik routerboard interface.

2.3 Data analysis

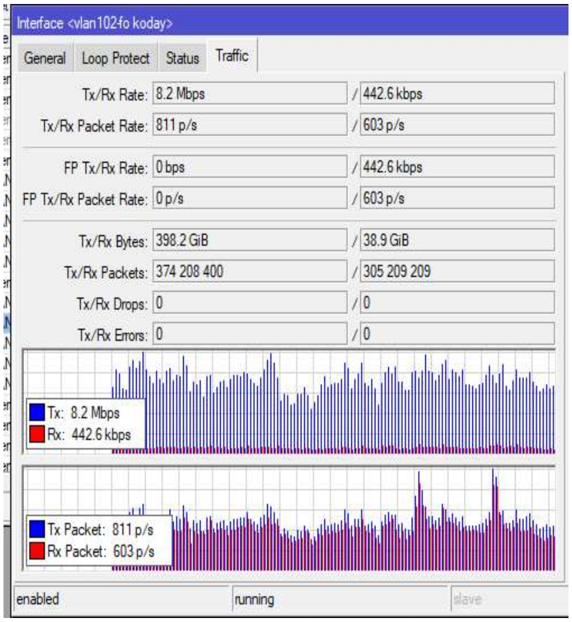
Data analysis at the location of DDoS attacks carried out for research is as follows :



R	ether2-trunk S1	Ethemet	1500	1592	19.9 Mbps	1856.6 kbps
R	vlan10-S1	VLAN	1500	1588	2.7 kbps	0 bps
R	vlan20-zte	VLAN	1500	1588	1876.0 kbps	93.1 kbps
R	vlan30-zte	VLAN	1500	1588	1884.1 kbps	75.4 kbps
R	vlan40-fo utara	VLAN	1500	1588	4.7 Mbps	742.0 kbps
R	vlan50-fo barat	VLAN	1500	1588	9.3 Mbps	735.1 kbps
R	ether3-trunk S2	Ethemet	1500	1592	24.2 Mbps	2.7 Mbps
R	vlan101-S2	VLAN	1500	1588	2.7 kbps	0 bps
R	vlan102-fo koday	VLAN	1500	1588	6.5 Mbps	540.8 kbps
R	vlan103-pbe m5 barat	VLAN	1500	1588	5.3 Mbps	321.4 kbps
R	vlan104-fo timur	VLAN	1500	1588	4.6 Mbps	307.5 kbps
R	vlan105-zte	VLAN	1500	1588	6.6 Mbps	1350.2 kbps
	ether8-console	Ethemet	1500	1592	0 bps	0 bps
	ether9-koday testing	Ethemet	1500	1592	0 bps	0 bps
R	ether10-al-manshuriah	Ethemet	1500	1592	5.8 Mbps	1257.7 kbps

Figure 2. Mikrotik interface

Figure 2. Shows 10 active mikrotik interfaces or 10 internet access sharing lines including 1).vlan20-ZTE, 2).vlan30-ZTE, 3).vlan40-north fo, 4).vlan50-west fo, 5).vlan102- fo koday, 6).vlan103-pbe m5 west, 7).vlan104-fo east, 8).vlan105-zte, 9).ether9-koday testing and lastly 10).ether10-al-manshuriah. These 10 paths are the paths that come out of mikrotik.



Interface <vlan102-fo koday>

Tx/Rx Rate: 8.2 Mbps / 442.6 kbps
Tx/Rx Packet Rate: 811 p/s / 603 p/s
FP Tx/Rx Rate: 0 bps / 442.6 kbps
FP Tx/Rx Packet Rate: 0 p/s / 603 p/s
Tx/Rx Bytes: 398.2 GiB / 38.9 GiB
Tx/Rx Packets: 374 208 400 / 305 209 209
Tx/Rx Drops: 0 / 0
Tx/Rx Errors: 0 / 0

enabled running slave

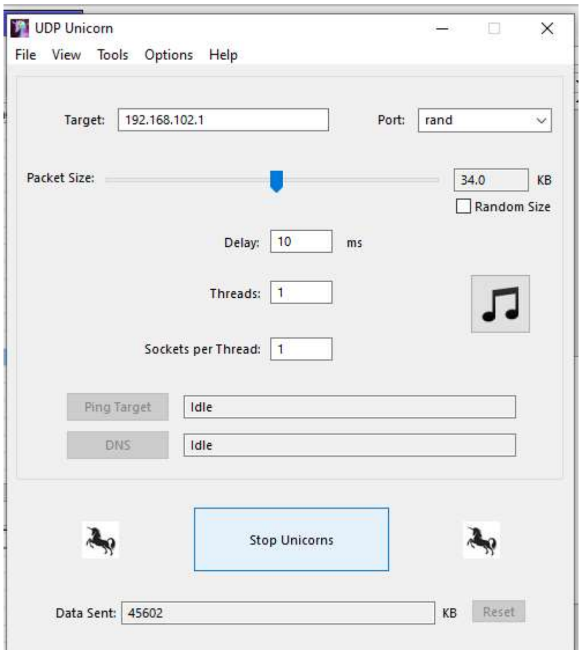
Figure 3. Interface <vlan102-fo koday>

Figure 3. Shows the <vlan102-fo koday> interface showing normal traffic and no DDoS attacks have occurred. The average download traffic is 8.2Mbps and the average upload traffic is 44.6kbps. The download result is greater than the upload result.

2.4 Unicorn UDP Attack Form

Figure 4. Shows UDP unicorn software by entering the server's IP address in the target column and providing the value of the packet size to be sent then clicking start unicorn to run a DDoS attack on the target

The forms of UDP Unicorn software attacks when used to carry out DDoS attacks are as follows :

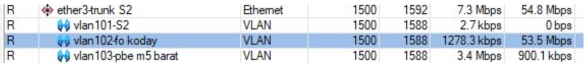


UDP Unicorn

Target: 192.168.102.1
Port: rand
Packet Size: 34.0 KB
□ Random Size
Delay: 10 ms
Threads: 1
Sockets per Thread: 1
Ping Target: Idle
DNS: Idle

Data Sent: 45602 KB

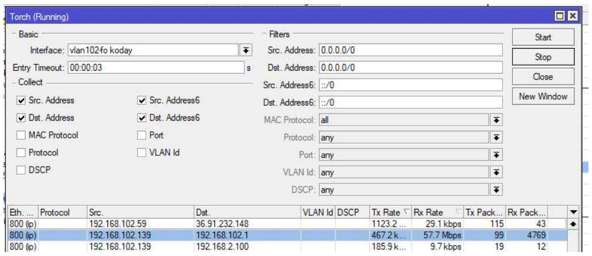
Figure 4. UDP Unicorn



R	ether3-trunk S2	Ethemet	1500	1592	7.3 Mbps	54.8 Mbps
R	vlan101-S2	VLAN	1500	1588	2.7 kbps	0 bps
R	vlan102-fo koday	VLAN	1500	1588	1278.3 kbps	53.5 Mbps
R	vlan103-pbe m5 barat	VLAN	1500	1588	3.4 Mbps	900.1 kbps

Figure 5. Unicorn UDP Attack

Figure 5. Shows an attack from the UDP unicorn software by filling up the upload traffic so that legitimate user traffic cannot access the internet. When an attack occurs, the monitored download traffic is 1278.3kbps while the monitored upload traffic is 53.5Mbps. An increase in unnatural upload traffic on this interface causes the internet connection to be slow, unable to connect to wireless devices, loginpage cannot appear.



Torch (Running)

Basic
Interface: vlan102-fo koday
Entry Timeout: 00:00:03 s

Collect
☑ Src. Address ☑ Src. Address6
☑ Dst. Address ☑ Dst. Address6
□ MAC Protocol □ Port
□ Protocol □ VLAN Id
□ DSCP

Filters
Src. Address: 0.0.0.0/0
Dst. Address: 0.0.0.0/0
Src. Address6: ::/0
Dst. Address6: ::/0
MAC Protocol: all
Protocol: any
Port: any
VLAN Id: any
DSCP: any

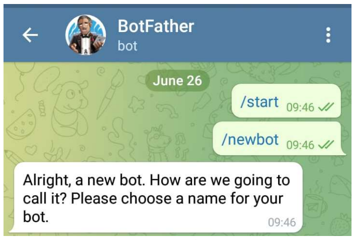
Eth. ...	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)		192.168.102.59	36.91.232.148			1123.2 ...	29.1 kbps	115	43
800 (ip)		192.168.102.139	192.168.102.1			467.2 k...	57.7 Mbps	99	4769
800 (ip)		192.168.102.139	192.168.2.100			185.9 k...	9.7 kbps	19	12

Figure 6. Mikrotik Torch Menu

Figure 6. Shows the torch menu on the Mikrotik router with the aim of knowing the IP address of the DDoS attacker by clicking start then shorting the highest Rx Rate. Figure 6 gets very high upload traffic with an average upload of 57.7Mbps.

2.5 DDoS Attack Detection and Mitigation System Design

The design of the DDoS attack detection and mitigation system using the telegram bot features as follows :



BotFather
bot

June 26

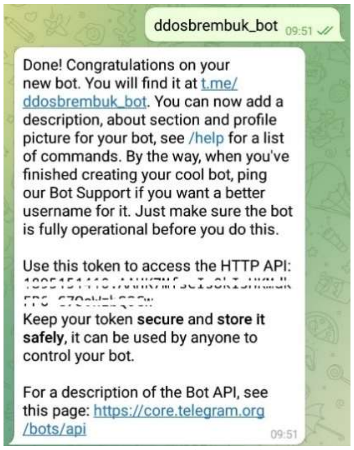
/start 09:46

/newbot 09:46

Alright, a new bot. How are we going to call it? Please choose a name for your bot. 09:46

Figure 7. BotFather Telegram

Figure 7. Shows the BotFather telegram that will be used as a telegram bot machine by writing the commands "/start" and "/newbot" to create a bot script.



ddosbrembuk_bot 09:51

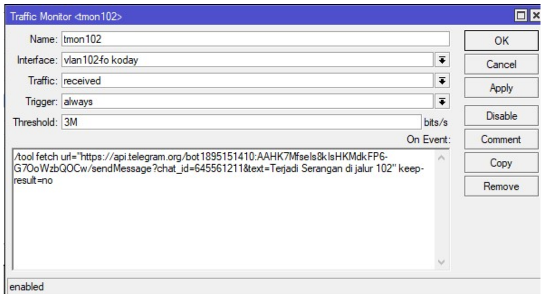
Done! Congratulations on your new bot. You will find it at t.me/ddosbrembuk_bot. You can now add a description, about section and profile picture for your bot, see /help for a list of commands. By the way, when you've finished creating your cool bot, ping our Bot Support if you want a better username for it. Just make sure the bot is fully operational before you do this.

Use this token to access the HTTP API:
[redacted]
Keep your token **secure** and **store it safely**, it can be used by anyone to control your bot.

For a description of the Bot API, see this page: https://core.telegram.org/bots/api 09:51

Figure 8. BotFather Telegram

Figure 8. Shows confirmation of the name of the bot, namely "ddosbrembuk_bot" which will be created to get a token to access the HTTP API telegram.



Traffic Monitor <tmon102>

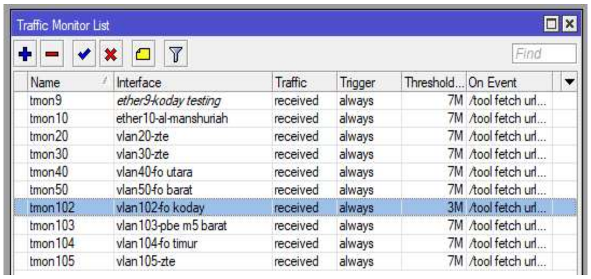
Name: tmon102
Interface: vlan102-fo koday
Traffic: received
Trigger: always
Threshold: 3M bits/s
On Event:

```
/tool fetch url="https://api.telegram.org/bot1895151410:AAHK7Mfsels8kIsHKMdkFP6-G7OoWzbQOCw/sendMessage?chat_id=645561211&text=Terjadi Serangan di jalur 102" keep-result=no
```

enabled

Fifure 9. Trafiic Monitor <tmon102>

Figure 9. Shows the existing monitor traffic on the proxy feature. With this traffic monitor it helps manual work when monitoring a DDoS attack that makes traffic very high. This monitor traffic menu is found in the Mikrotik tools when opening Winbox. The name column fills in the name tmon102 in order to provide a different name. The interface column selects the interface to be monitored. The traffic column uses received with the aim of monitoring traffic only on uploads. The trigger column uses always with the aim of always reporting all monitoring traffic activities. The threshold column provides a value of 3Mbps with the aim that if the upload traffic exceeds 3Mbps, it will report to the Telegram bot. The on event column adds a telegram bot script by entering the telegram bot token that has been obtained in the previous stage. The script will display a notification in real time on telegram with the message "An attack occurred on Line 102"



Traffic Monitor List

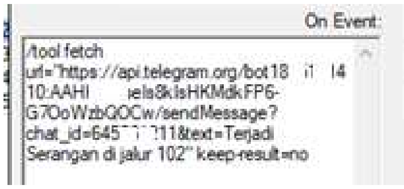
Name	Interface	Traffic	Trigger	Threshold...	On Event
tmon9	*ether9-koday testing*	received	always	7M	/tool fetch url...
tmon10	ether10-al-manshuriah	received	always	7M	/tool fetch url...
tmon20	vlan20-zte	received	always	7M	/tool fetch url...
tmon30	vlan30-zte	received	always	7M	/tool fetch url...
tmon40	vlan40-fo utara	received	always	7M	/tool fetch url...
tmon50	vlan50-fo barat	received	always	7M	/tool fetch url...
tmon102	vlan102-fo koday	received	always	3M	/tool fetch url...
tmon103	vlan103-pbe m5 barat	received	always	7M	/tool fetch url...
tmon104	vlan104-fo timur	received	always	7M	/tool fetch url...
tmon105	vlan105-zte	received	always	7M	/tool fetch url...

Figure 10. Traffic Monitor List

Figure 10. Shows a list of monitor traffic. In the picture there are 10 internet access sharing lines that will be monitored for upload traffic to mitigate ongoing DDoS attacks. The results of this script will immediately make a real-time notification to Telegram in the event of a DDoS attack. In the name column, fill in the name and adjust it to the monitored path so that it provides a different name and in the threshold column it adjusts to the maximum desired upload speed.

III. RESULTS AND DISCUSSION

The results and discussion of DDoS attack mitigation using telegram are as follows :

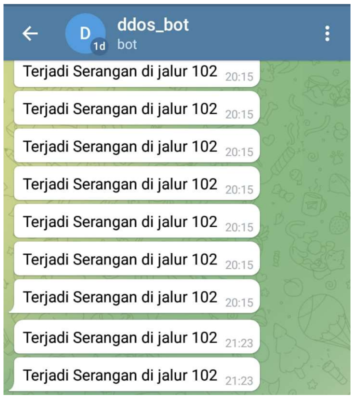


On Event:

```
/tool fetch
url="https://api.telegram.org/bot18   i1   l4
10:AAHI       jels8kIsHKMdkFP6-
G7OoWzbQOCw/sendMessage?
chat_id=645     11&text=Terjadi
Serangan di jalur 102" keep-result=no
```

Figure 11. Script On Event

Figure 11. shows this script generated with BotFather from the telegram bot by forwarding the url and chat_id links embedded in the script, as follows: url=https://api.telegram.org/bot18951410:AAHK7MfseIs8kIsP6-G7OoWzbw, chat_id=645211. Then give a comment or notification in the form of text = An attack occurred on line 102.



ddos_bot
bot

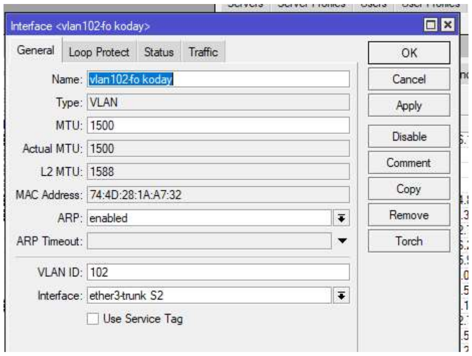
Terjadi Serangan di jalur 102 20:15
Terjadi Serangan di jalur 102 20:15
Terjadi Serangan di jalur 102 20:15
Terjadi Serangan di jalur 102 20:15
Terjadi Serangan di jalur 102 20:15
Terjadi Serangan di jalur 102 20:15
Terjadi Serangan di jalur 102 20:15
Terjadi Serangan di jalur 102 21:23
Terjadi Serangan di jalur 102 21:23

Figure 12. DDoS Attack Notification Results

Figure 12. Shows the results of realtime DDoS attack notifications when there is a spike in upload data traffic. If there is data traffic that exceeds the value above 3Mbps, a notification will be sent to the Telegram application according to the 3Mbps upload/threshold value setting in Figure 9. If there are notifications that

enter the Telegram application more than 10 times within one second, it means that a DDoS attack has occurred.

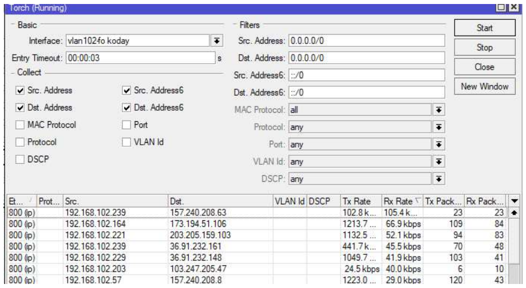
After knowing which internet connection line is being attacked, the first step is to immediately take action by tracing the user using the torch feature on the Mikrotik routerboard interface menu.



Name: vlan102-fo koday
Type: VLAN
MTU: 1500
Actual MTU: 1500
L2 MTU: 1588
MAC Address: 74:4D:28:1A:A7:32
ARP: enabled
ARP Timeout:
VLAN ID: 102
Interface: ether3-trunk S2
□ Use Service Tag

Figure 13. Unlock Torch Features

Figure 13. Shows how to open the torch feature by clicking the interface menu → then clicking the torch feature.



Interface: vlan102-fo koday
Entry Timeout: 00:00:03 s

☑ Src. Address
☑ Dst. Address
□ MAC Protocol
□ Protocol
□ DSCP
☑ Src. Address6
☑ Dst. Address6
□ Port
□ VLAN Id

Src. Address: 0.0.0.0/0
Dst. Address: 0.0.0.0/0
Src. Address6: ::/0
Dst. Address6: ::/0
MAC Protocol: all
Protocol: any
Port: any
VLAN Id: any
DSCP: any

Et...	Prot...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)		192.168.102.239	157.240.208.63			102.8 k...	105.4 k...	23	23
800 (ip)		192.168.102.164	173.194.51.106			1213.7 ...	66.9 kbps	109	84
800 (ip)		192.168.102.221	203.205.159.103			1132.5 ...	52.1 kbps	94	83
800 (ip)		192.168.102.239	36.91.232.161			441.7 k...	45.5 kbps	70	48
800 (ip)		192.168.102.229	36.91.232.148			1049.7 ...	41.9 kbps	103	41
800 (ip)		192.168.102.203	103.247.205.47			24.5 kbps	40.0 kbps	6	10
800 (ip)		192.168.102.57	157.240.208.8			1223.0 ...	29.0 kbps	120	43

Figure 14. Torch Feature

Figure 14. Shows the torch feature, with this feature it is easy to see data traffic (Tx/Rx) which can be sorted from the largest to the smallest. To see the attacker by looking at the source address and sorting the upload data traffic (Rx) from the largest to the smallest.

Then with the second step, trace the internet connection path using wired or wireless transmission media by removing the RJ45 connector connected to each computer network device, and ensuring always monitoring the Mikrotik interface from Winbox.

IV. CONCLUSION

The conclusion of this research is: 1) There was a DDoS attack using UDP unicorn software which resulted in a traffic spike of 53.5 Mbps on the upload traffic side which resulted in slow traffic of legitimate/authenticated users. 2) By using telegram bots to know DDoS attacks occur in real time with a success rate of attack detection up to 100% notifications on telegram bots. Mitigation of DDoS attack mitigation as soon as possible take steps a) take action to track users using the torch feature on the Mikrotik routerboard interface menu by clicking the interface menu where the attack occurred and then clicking the Torch feature. b) trace the internet connection path using wired or wireless transmission media by removing the rj45 connector connected to each computer network device (router/switch), as well as ensuring always monitoring the proxy interface from winbox.

REFERENCES

[1] Kabayankababayan, “Mengenal Bot Telegram,” 2015. https://rizaumami.github.io/2015/12/11/mengenal-bot-telegram/ (accessed Dec. 01, 2021).

[2] N. Sugianti, Y. Galuh, S. Fatia, and K. F. H. Holle, “Deteksi Serangan Distributed Denial of Services (DDOS) Berbasis HTTP Menggunakan Metode Fuzzy Sugeno,” *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 4, no. 3, pp. 156–164, 2020, doi: 10.14421/jiska.2020.43-03.

[3] J. C. J. Sihombing, D. P. Kartikasari, and A. Bhawiyuga, “Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software-Defined Network (SDN),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 10, pp. 9608–9613, 2019.

[4] M. Aziz, R. Umar, and F. Ridho, “Implemetasi Jaringan Saraf Tiruan untuk Mendeteksi Serangan DDoS pada Forensik Jaringan,” *QUERY J. Sist. Inf.*, vol. 3, no. 1, pp. 46–52, 2019.

[5] E. P. Nugroho, E. Nugraha, and M. N. Zulfikar, “Sistem Reporting Keamanan pada Jaringan Cloud Computing Melalui bot Telegram dengan Menggunakan Teknik Intrussion Detection and Prevention System,” *J. Teknol. Terpadu*, vol. 5, no. 2, pp. 49–57, 2019, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JTT/article/view/233.

[6] J. Fahana, R. Umar, and F. Ridho, “Pemanfaatan Telegram sebagai Notifikasi Serangan untuk Jaringan Forensik,” *Query J. Inf. Syst.*, vol. 1, no. 2, pp. 6–14, 2017, [Online]. Available: http://jurnal.uinsu.ac.id/index.php/query/article/view/1036.

[7] D. Ariyus, *INTRUSION DETECTION SYSTEM: Sistem Deteksi Penyusupan Pada Jaringan Komputer*. Yogyakarta: Andi, 2007.

[8] S. M. Mousavi, “Early Detection of DDoS Attacks in Software Defined Networks Controller,” in *Thesis*, Ottawa, 2014, pp. 77–81.

[9] S. kumarasamy and R. Asokan, “Distributed Denial of Service (DDOS) Attacks Detection Mechanism,” *Int. J. Comput. Sci. Eng. Inf. Technol.*, vol. 1, no. 5, pp. 39–49, 2011, doi: 10.5121/ijcseit.2011.1504.

[10] A. Chopra, “Security Issues of Firewall,” *Int. J. P2P Netw. Trends Technol.*, vol. 22, no. 1, pp. 4–9, 2016, doi: 10.14445/22492615/ijptt-v22p402.

[11] citraweb, “Traffic Monitor Mikrotik,” *mikrotik.id*. https://mikrotik.id/artikel_lihat.php?id=289 (accessed Aug. 11, 2021).

[12] S. R. Umami, “Mengenal Bot Telegram,” *2015*, 2015. https://rizaumami.github.io/2015/12/11/mengenal-bot-telegram/ (accessed Aug. 11, 2021).