Saurabh Lakhe et al. 2016, Volume 4 Issue 2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Detection of Distributed Denial of Service Attacks and Mitigating the Effect of the Attack

[1]Akash Ukande, [2]Avin Vij, [3]Saurabh Lakhe, [4]Shubham Gedam, [5]Sumit Ishwarkar

Abstract

In the world of computer network, the distributed denial of service attacks have become one of the most harmful attacks on the networks services. Hence there is a need to design effective mechanisms to detect and mitigate the effect of these attacks. In this paper, we propose to detect the various DDoS attacks like TCP Flood, TCP SYN-FIN, Port 0 attacks by analyzing the packet headers against the well defined rules and conditions. Detected attack packets will be separated from normal traffic packets and the effect of attack traffic will be mitigated by the mitigation mechanism. The performance of victim and designed detection and mitigation mechanisms under various attack patterns will be evaluated using evaluation parameters- CPU usage and memory usage, response time.

Keywords: DDoS attacks; Detection; Mitigation; CPU usage; Response Time

Introduction

A denial of service attack is an attempt towards a machine or network resource unavailable to its intended or legitimate users, such as to temporarily or indefinitely interrupt services of a host connected to the internet. A distributed denial of service is where the attack source is more than one, often thousands of, unique IP addresses. It is similar to a group of people crowding the entry door of a shop, and not allowing legitimate customers enter into the shop, thus disrupting normal operations. There are various types of DDoS attacks like TCP flood attack, TCP SYN-FIN attack, Port 0 attack and many more.

It is very important to detect such attacks fast and accurately at the server side. The main purpose of DDoS attacks is to exhaust host resources and choke the bandwidth. Thus during detection, looking at the CPU usage and memory usage of the victim machine, it is essential to reduce the detection time.

The defense mechanism involves dropping and thus stopping the malicious packets from processing. The malicious packets are the invalid packets whose flag settings and the other parameters like source and destination IP addresses, source and destination port numbers, protocol have been intentionally altered by the attackers.

These invalid packets aim to make the resources unavailable to the legitimate users. If such packets are allowed to process on the victim machine that is the server, then they are harmful enough to deny the services that the server provides.

The defense mechanism activates once the detection mechanism has done its job of detecting the malicious packets. The importance of defense mechanism is to drop all such packets and thus, not allow them to process on the server machine.

Related work

DDoS that is Distributed Denial of Service attack is a form of attack where a lot of computers are used to flood the targeted servers – victim, that has a huge amount of information and choke it in order to prevent it' s genuine users from accessing the service (mostly web servers that host websites). In some cases, the web servers with huge traffic are flooded in a periodic manner in order to degrade their service, instead of taking it down completely. The components and architecture of DDoS attack is given:

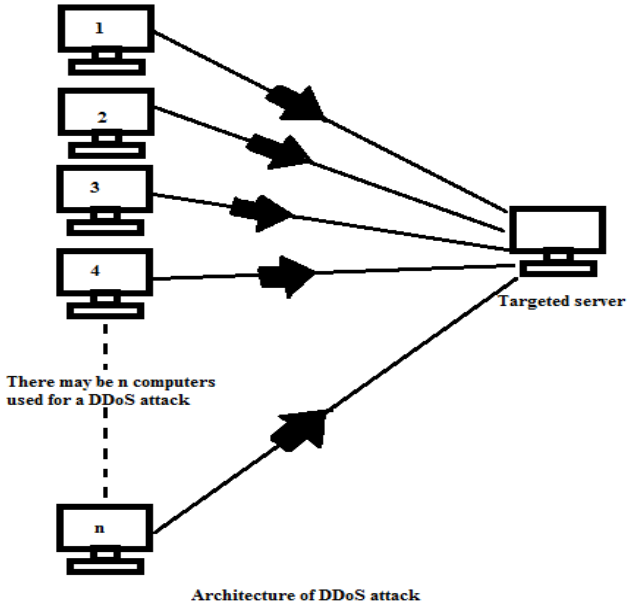

Figure 1: Architecture of DDoS attack

The above architecture diagram represents Distributed Denial of Service attack, there are two main components that are always there – The attacker computer from where the attacks are initiated and the victim server which comes under the attack. The presence of these two components makes the attack denial of service attack.

Similarly, simultaneous attack from several computers on to the targeted server makes it a Distributed denial of service attacks.

Types of attacks

SYN Flood:

A SYN flood DDoS attack violates the sequence of the "three-way handshake" concept where a SYN (Synchronize) request is used to initiate a TCP connection with a server. Which then must be acknowledged by a SYN-ACK response from that server, and then confirmed by an ACK response from the initiator. In a SYN flood scenario, the sender sends multiple SYN (Synchronize) requests, but does not respond to the server's SYN-ACK response, and further sends the SYN requests from the spoofed IP address from the same machine. Meanwhile, the server system continues to wait for acknowledgement for each of the requests, thus binding resources due to which no new connections can be established, and ultimately results in choking of the service hence the denial of service.

Port 0 attack:

The valid range of TCP port number lies from 1 to 65535. If any of the port involved in the TCP connection that is port number of source machine and the port number of destination machine possesses port number "zero", then it will be classified as a port 0 attack.

SYN-RST attack:

The function of SYN flag is to initiate a connection by requesting a SYN request to the host when the flag is set. On the other hand, the objective of the RST flag is to reset the connection when the flag is set. When these two flag are set together then conceptually this is invalid and ultimately results as a denial of service attack.

SYN-ACK attack:

The function of SYN flag is to initiate a connection by requesting a SYN request to the host when the flag is set. While the objective of ACK flag is to respond to the received SYN flag. If both the flags are set together, then it will result as an invalid flag setting which violates the sequence of the three way handshake concept. This is also one type of denial of service attack which attacker performs.

SYN-FIN attack:

The function of SYN flag is to initiate a connection by requesting a SYN request to the host when the flag is set. While FIN flag stands for releasing the established connection. When these two flags are set together then conceptually this is invalid and results as a denial of service attack.

URG-FIN-PSH attack:

FIN flag stands for releasing the established connection when it is set. PSH flag stands for pushing the data when it is set. URG flag stands for specifying the offset from sequence number indicating the last urgent data byte. When all these three flags are set together then it is an invalid flag setting in a connection and hence results as a denial of service attack.

Design model

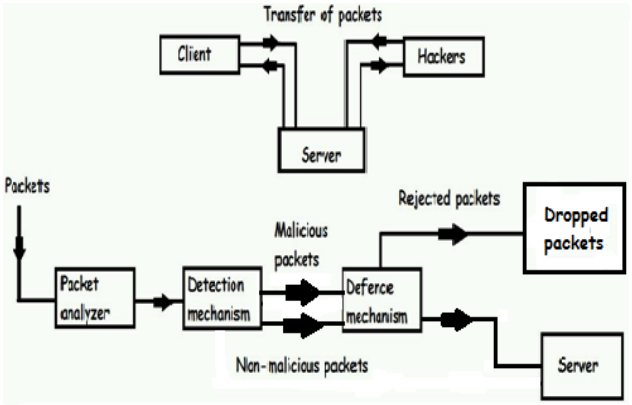

Figure 2: Design model of the project

Information is passed on the web through the packets. Now there may be legitimate users those intend to obtain the resources and services provided by the server while there may be non-legitimate users that are the attackers whose prime objective is to deny the services available to the valid users.

The packets that are sent to the server are analyzed using the Packet analyzer tools that gives the information about the various parameters of the packets like the protocol, source port number, destination port number, various flag settings, number of packets, source IP address, destination IP address.

Further the detection mechanism designed differentiates between malicious and non-malicious packets depending on the various flag settings, valid-invalid IP address, valid-invalid port number of source and destination.

All such distinguished packets are passed to the defense mechanism that has is the power to stop all the malicious (invalid) packets from processing on the server machine. Defense mechanism send non-malicious packets to the server and all malicious (invalid) packets are dropped by the defense mechanism.

Working procedure

Client – server configuration module

In this module, we have created a client-server environment .For the purpose of making a machine server, we have used Apache Tomcat server as the server software. We installed this software on one of the machines and configured the .xml files such as server.xml, web.xml, config.xml, tomcat-users.xml. These changes were made in order to setup a server – client environment. All the other computers are connected to the server machine and thus they act as clients.

Attacker module

DDoS attacks consist of n number of machines that can act as attackers on the server machine. Thus, we have used Packet Building softwares that help us to send packets to the server once the clients and server are in a connection via the Lan cables. The various packet building tools allow us to choose the network interface and to set source and destination IP addresses, source and destination ports and various TCP flag settings like RST, FIN, URG, PSH, SYN. Further the attackers can choose the protocol depending on the type of DDoS attack they want to perform and also set the number of packets that they intend to send. In the attacker module, we have mainly considered TCP protocol as the type for DDoS attacks. Thousands and lakhs of packets can be sent from a machine to another machine. This number of packets can be considered to be enough so as to flood the server machine thus resulting in thousands and lakhs of half open connections which denies the other users to request for a connection in order to use its resources. Various combinations of flags settings can be used that will question its validity conceptually. Combination like SYN-FIN is an invalid flag setting as it means requesting the server for a connection and at the same time requesting it for a termination of that connection. Hence many other invalid combinations of flags can prove to be harmful enough to cause a DDoS attack.

Packet capturing module

In this module, we dealt with the capturing of packets that were sent to the server from various attacker machines. This module is created in order to get notified about the type of packets and its various parameters. Such modules provide the details of the captured packets and show information like the source IP address, destination IP address, source port number, destination port number, protocol of the packet, its various flag settings.

For each and every packet received by the server, the algorithm will scan packet depending on some parameters such as valid flag settings for the TCP packets, length of the UDP packets, etc. If these parameters match to the standard parameters of the respective protocol then they are termed as /genuine

packets. If not, they will be termed as malicious packets.

Detection module

The prime objective of detection algorithm is to detect and distinguish between malicious and non-malicious packets. The packet sniffer does its job by giving useful information about the receiving packets. With the help of this information, detection module is able to detect the packets with invalid parameters to term them as malicious.

This will help the defense mechanism to restrict those packets that are malicious as termed by the detection mechanism.

The flowchart for the detection module is shown:

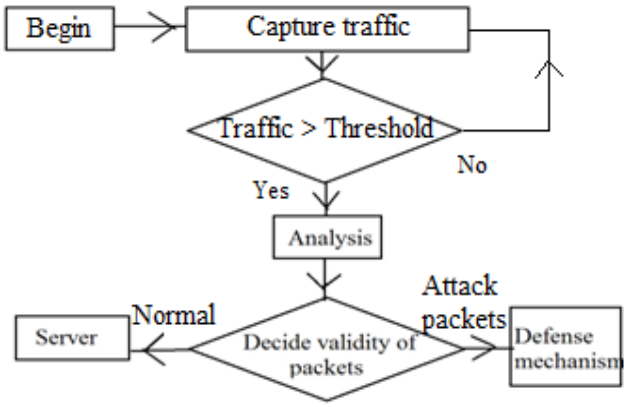

Figure 3: Flowchart of detection module

The algorithm for the detection module is mentioned below:

1) Start

2) Accept every incoming packet as the input

3) Check the source and destination IP addresses, source port and destination ports, protocol of the packet, its various flag settings

3.1) IF normal packets, check for its flooding (whether normal packets are sent over and over again)

3.2) IF attack packets, forward them into the defense mechanism.

Consequently one needs to check the CPU usage and memory usage of the server machine as it abruptly increases because that is the effect of DDoS attack for TCP protocol. For a normal state of the server machine where it is not under any attack, the CPU and memory usage may vary between 5-10% and 1.50-2.0GB respectively depending on the processes going on. Once the server is under attack, the CPU and memory usage rapidly increases upto 80%, which slows down the machine and hangs it.

Defense module

The malicious packets are passed through the defense mechanism. The malicious packets are dropped and non-malicious packets are prompted to the server for further processing. The algorithm for the defense module:

1) Note response time of overall detection mechanism

1.1) Check the CPU and memory usage for three circumstances

1.1.1) before attack

1.1.2) during attack

1.1.3) after applying the detection mechanism

2) When to trigger defense mechanism (if threshold is passed)

3) Any attack packet is dropped

3.1) most drop conditions are fulfilled by detection mechanism

4) Packets dropped are analyzed i.e.

i) How many packets were dropped?

ii) Why these packets were dropped?

The response time of detection mechanism is an important parameter to judge the efficiency and reactivity of the mechanism. There are other evaluation parameters like CPU usage, memory which can be the effects of the DDoS attack like sudden increase in CPU and memory utilization that causes problem to the server machine. Once the defense mechanism is activated, the increased CPU usage memory usage should decline and come to normal state.

Evaluation and result

Graphical study

The observations done during the complete performance of the project needs a graphical representation. The graph for various types of attacks is plotted. It consist time interval being plotted on the x-axis while number of packets being plotted on the y-axis. The graphical representation is given below:

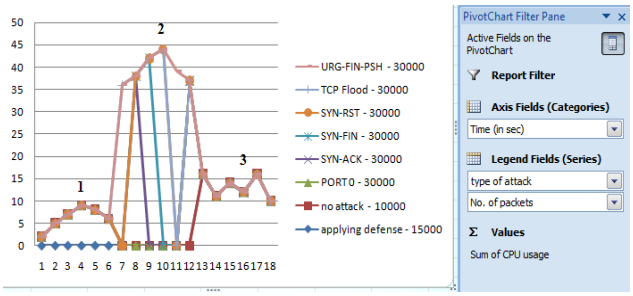

Figure 4: Graph of different attack state

A. Region 1 depicts state before attack where the cpu usage of the server machine is normal in the range of 5-10 %.

B. Region 2 depicts state during attack where the CPU usage of the server machine is very high in the range of 42-56%.

C. Region 3 depicts state after attack with the defense mechanism activated where the CPU usage of the server machine declines and comes to the normal range of 10-16%.

Attack without defense mechanism

There are various evaluation parameters like CPU usage memory usage and response time on the basis of what we can see the effects of the DDoS attacks on the server machine. The result involves the GUI(Graphical user interface) that gives the description of the receiving packets like source port number, destination port number, source IP address, destination IP address, protocol, flags, reason for which the packet must be dropped. Also, it involves the CPU usage and memory usage which can be seen in the task manager. Now, during the attack when the defense mechanism is not active, the CPU usage and memory usage increases abruptly .This causes the server machine to slow down and ultimately it is unable to provide the services to its legitimate users. The GUI created gives the reason for which the packet must be dropped.

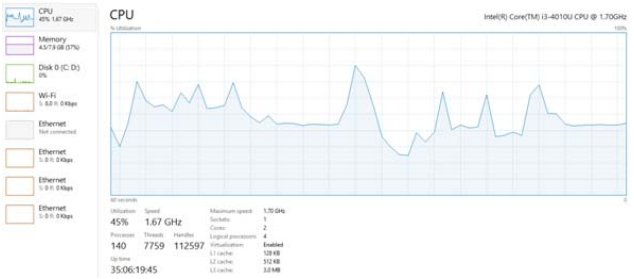

Figure 5: CPU graph during attack

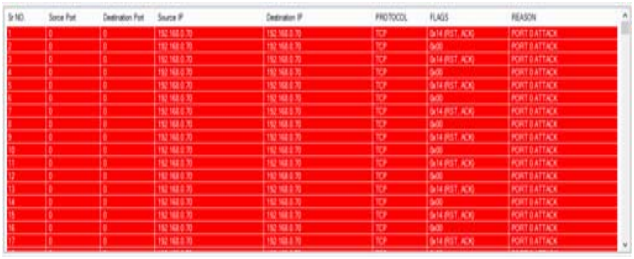

Figure 6: Detection module showing attack

The above picture shows the CPU usage that reaches up to 45% which is more than the normal state.

Attack with defense mechanism

Most the parameters of the receiving packets are given by the detection mechanism. Hence, the defense mechanism has enough reasons to drop the invalid packets.

The GUI created has the option of activating the defense mechanism. Once it is activated by checking the box, it will drop all the malicious packets. The reason for dropping the packets is mentioned in the GUI. If the defense mechanism is activated during the attack, the CPU and memory usage declines up to 10-15%. The following picture gives experimental view:

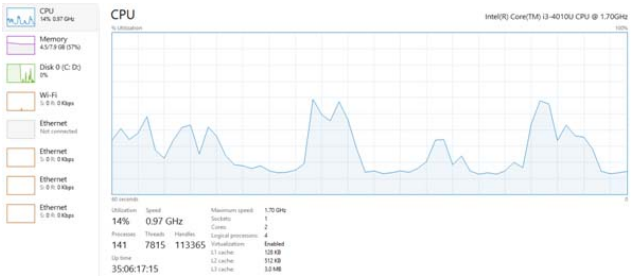

Figure 7: CPU graph when defense is on

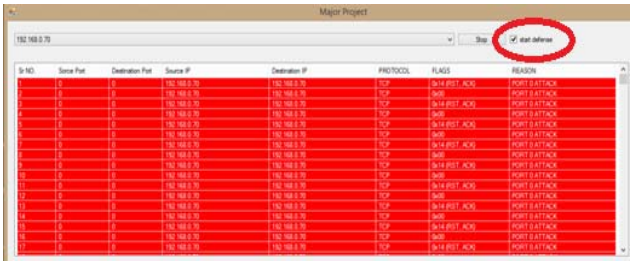

Figure 8: Attack with defense mechanism

There is another important parameter namely response time which indicates how reactive is the designed mechanism. Response time is the time required by the mechanisms to react when the server machine is under attack. Practically, it is observed that the value is quite less (in nanoseconds). The response time is directly proportional to the reactivity of the mechanism designed. Hence, lesser the response time better it is for the server to avoid any DDoS attack for the most part.

Tabular representation

Table 1: CPU usage with respect to attack state

Serial no	CPU usage	Attack state
1	5-10%	No
2	42-56%	Yes
3	10-15%	Yes with defense mechanism on

The table 1 represents the data about the evaluation parameters namely, CPU utilization. For the different attack states, the CPU utilization varies abruptly.

Conclusion

Today, maximum people rely on network services, so the resistibility to DDoS attack has become one of the most pivotal sections to service providers. This paper possesses an effective method of handling and securing the resources by detection and defense mechanism against various types of DDoS attacks. By deploying detection mechanism, the classification of malicious and non-malicious packet has been done on the basis of various valid and invalid conditions. While by defense mechanism we restrict the malicious packet from reaching towards the server and dropped them.

For future work, efforts will be made for tracking MAC address which act as a pivotal factor in case of performance measure. Hence statically located IP address could also be traced. So, that in future when the packets are received from the same IP address then they will be dropped directly and that IP address will be blacklisted.

References

[1] J. Mirkovic, J. Martin, and P. Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms",2004

[2] Sirikarn Pukkawanna, Vasaka Visoottiviseth, Panita Pongpaibool," Lightweight Detection of DoS Attacks",2007

[3] Shuyuan Jin , Daniel S. Yeung," A Covariance Analysis Model for DDoS Attack Detection",2004

[4] Yi Zhang,Qiang Liu, Guofeng Zhao , "A Real-Time DDoS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis",2010

[5] Jelena Mirkovic , Gregory Pier ,Peter Reiher, "Attacking DDoS at the source" ,2002

[6] T. Peng, C. Leckie and R. Kotagiri, "Survey of network-based defense mechanisms countering the DoS and DDoS problems", ACM Comput. Surv. 39, April 2007.

[7] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of service attack detection techniques," IEEE Internet Computing, vol.10, no. 1, 2006, pp. 82-89.

[8] M. Thottan and J. Chuanyi, "Anomaly detection in ip networks," IEEE Trans. on Signal Processing, vol. 51, no. 8, 2003, pp. 2191-2204.

[9] Y.Ohsita, S. Ata, and M. Murate. Detecting distributed denial-of-service attacks by analyzing TCP SYN packets statistically. In IEEE GlobalTelecommunications Conf. 2004, pp. 2043-2049.

[10] Haining Wang, Danlu Zhang and Kang G. Shin, "Detecting SYN Flooding Attacks", IEEE INFOCOM 2002, New York City, June 2002.

[11] Editorial, "Distributed Denial-of-service and Intrusion Detection," Journal of Network and Computer Applications, vol. 30, 2007, pp. 819- 822.

[12] J.Oh, J. Hwang, and Y. Han, "A packet-by-packet scheduling algorithm for wireless multimedia systems," in IEEE 66th Vehicular TechnologyConf. IEEE, Oct 2007.

[13] Lau, F., Rubin, S.H., Smith, M.H., Trajovic, L.: Distributed denial of service attacks. In: IEEE International Conference on Systems, Man, and Cybernetics, pp. 2275-2280, Nashville/USA, 2000.

[14] Hemant Sengar, Xinyuan Wang, Haining Wang, Duminda Wijesekera and Sushil Jajodia, "Online Detection of Network Traffic Anomalies Using Behavioral Distance", IEEE IWQoS 2009 , Charleston,July2009.

Author's details

[1,2,3,4,5] Student, Computer Technology, Yeshwantrao Chavan College of engineering, Maharashtra, India.

Email: [1]akashukande44@gmail.com, [2]avinvij26@gmail.com, [3]saurabhlakhe2310@gmail.com, [4]gedamshubham@gmail.com, [5]sumish281995@gmail.com

Copy for Cite this Article- Akash Ukande, Avin Vij, Saurabh Lakhe, Shubham Gedam and Sumit Ishwarkar, "Detection of Distributed Denial of Service Attacks and Mitigating the Effect of the Attack", *International Journal of Science, Engineering and Technology,* Volume 4 Issue 2: 2016, pp. 414- 420.