Security Against DDoS Attack

Jogin Joshi#1, Dr. Dhaval Parikh#2

#1Scholar, Computer Engineering Department, GEC, Gandhinagar, India.
#2Professor & HOD, Computer Engineering Department, GEC, Gandhinagar, India

---***---

Abstract - *There are various services available to the users from business perspective over the internet. For any service it's availability is very important. DDoS is an attack which hampers the availability of a service. DDoS is an acronym of Distributed Denial of Service. It is an attack where many malicious network nodes sends huge volume of unnecessary traffic to make the service down. There are mainly two types of DDoS attack based on the protocol layers on which they corresponds. The transport layer attacks like TCP, UDP flooding are example of transport layer DDoS attacks and HTTP fragmentation attack, DNS reflection attack etc are example of application layer DDoS attack. There are various techniques to defend and mitigate DDoS attacks like rate limiting, stateful packet inspection, CAPTCHA, ingress-egress filtering etc but each can defend only specific layered attack or specific attack. So we need to have integrated technique to defend multilayered attack. and achieve desired availability of a service.*

Keywords: DDoS, Detection, Prevention, Mitigation, Flooding, TCP, UDP, ICMP

1. INTRODUCTION

Service availability states how much time service is available from the total time and hence availability of a service is very important for any consumable service. DDoS is an attack where malicious requests are sent to the victim service and due to overwhelming traffic and resulting high consumption of resources makes the service slow or unavailable.[3]

DDoS is known as one of the most affecting attacks to business and service availability. Daily thousands of such attacks are evident in the internet.[3] The target service are ISPs, e-commerce sites, banks and other commercial organizations majorly.[7]

2. OVERVIEW OF DDOS ATTACKS

2.1 DDoS Motives

There are various motives behind DDoS attacks but the major intention is to make the victim service unavailable and let them suffer financial loss. The major motives are as below:

1) Financial benefits: The intention here is to incur financial loss due to unavailability of service. [7]

2) Revenge: There are incidents where personal or professional revenge are the reason behind such attacks. [7]

3) Ideological differences: Ideological or religious beliefs are sometimes causes of such attacks.[7]

4) Intellectual challenge: Few attackers wants to show their capabilities by initiating DDoS attacks. [7]

5) Cyberwar : Sometimes military organization or terrorists tries to attack some reputed organizations of other country to make negative impacts on them. [7]

2.2 Types of DDoS Attack

DDoS attacks are mainly classified into two major types as below:

1) Network/transport layer attacks: This type of attacks operates on network or transport layer. SYN flooding, UDP flooding, ICMP Smurf, etc are examples of such attacks. There are more common attacks happening worldwide. [3][6]

2) Application layer attacks: This type of attacks operates on application layer and tries to diminish or crash the corresponding application. DNS Amplification, HTTP fragmentation etc are examples of this type of attacks. [3][6]

2.2 Examples of DDoS Attacks

1) Smurf Attack: In this type of attack entire network is used to generate huge volume of traffic and redirects it to victim machine which makes the service unavailable. [6]

2) HTTP Flood Attack: In this type of attack huge volume of HTTP GET and POST requests are sent to the victim service on valid TCP connection. It consumes the computing resources of the victim machines and makes the service unavailable. [7]

3) UDP Flood Attack*:* In this type of attack a huge count of UDP packets are targeted to the victim machine. The victim machine continuously checks for any available service and replies with "ICMP Host Unreachable" packet. Due to excessive flow of such requests and continuous checks makes the service unavailable. [7]

5) SYN Flood Attack: TCP connection making follows three way handshaking protocol where first SYN request is sent, server replies with SYN-ACK and then client replies with ACK and thus the connection gets created. Here in this attack spoofed SYN requests are sent, server replies with SYN-ACK but then no ACK from clients makes the connection half-open and after a while connections exhausts completely. [6][7]

3. MITIGATION AND DEFENSE TECHNIQUES

3.1. Rate Limiting

Rate limiting as the name suggests limits the rate of the packets based on some pre-defined criteria like source or destination address or port etc. Due to regulation on traffic it defends DDoS attack and protects the victim machine. [1]

2.2. Ingress and Egress Filtering

Ingress filtering works on inbound traffic of the packets and do filtering and egress works on filtering outbound traffic which effectively drops traffic from unknown network. [1]

2.3. CAPTCHA based defense

CAPTCHA is an acronym of Completely Automated Public Turing Test to tell Computer and Humans Apart. Here, challenge and response mechanism is used to check and differentiate human and bots effectively. [2]

2.4. Software puzzle based problem

It is similar to CAPTCHA based technique but here puzzle is used to differentiate between humans and bots because only human can solve the puzzle effectively and this way we can identify and drop the bot's traffic. [2]

3. PROPOSED METHOD

There are multiple layers on which DDoS attack targets victim service. We have mitigation techniques but they work on individual attacks or individual layer attacks so we need an integrated approach to defend multiple layered DDoS attack. Here, we have devised an integrated approach where rate limiting, ingress egress filtering and CAPTCHA based techniques works in integrated and cohesive fashion to defend multi layered attacks.

3.1. SYSTEM FLOW

The proposed method has below steps to counter DDoS attacks:

- Apply ingress - egress filtering to filter unknown network
- Apply rate limit to drop all overrated packets
- Redirect request to transparent proxy
- Redirect to apache – tomcat for captcha based authentication
- On successful captcha authentication – redirect to service login page
- On successful login accept traffic and let them access service

3.2. COMPONENT VIEW

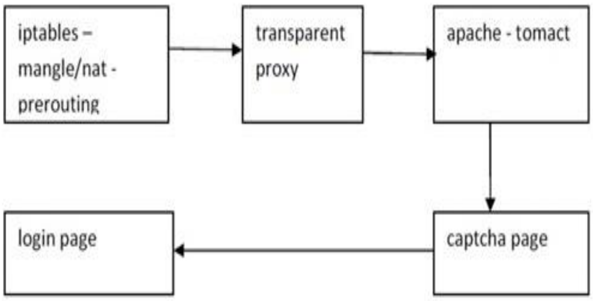

Fig-1. Component flow for proposed system

4. EXPERIMENT

• In the experiment, the web application is targeted for flooding attacks using a linux system with hping command

• Another system is used to generate application layer attacks using java based custom code.

• Here a system is used to monitor the performance of web application and to note the observations based on various techniques ingress, egress filtering, port filtering, rate limiting and hybrid techniques.

• The observations are then taken, averaged and noted.

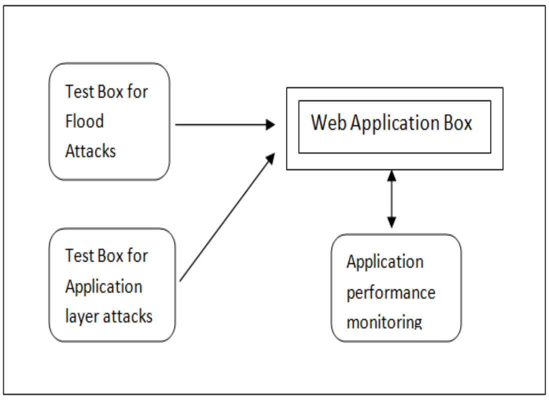
Test Box for Flood Attacks
Web Application Box
Test Box for Application layer attacks
Application performance monitoring

Fig-2: Experiment setup of the system

4.1. System configuration

4.1.1. Web Application Box - Virtual machine

Intel Core i3 CPU 2.2 GHz

3 GB RAM

Fedora Linux OS

4.1.2. Test Box for Flood Attacks - Virtual machine

Intel Core i3 CPU 2.2 GHz

2 GB RAM

Fedora Linux OS

4.1.3. Test Box for Application layer Attacks - Virtual machine

Intel Core i3 CPU 2.2 GHz

2 GB RAM

Fedora Linux OS

5. RESULTS

The experiment was carried out on a web application installed on web application system based on linux. Below are the terms used to evaluate results of the experiments:

- RPS - It stands for request per second. It indicates input request flow to the service.
- Load Average – It show utilization of server in terms of how many processes are waiting so lower the count better the system health.
- % CPU – It shows the percentage utilization of CPU's of a system.
- % Memory - It indicates percentage utilization of the memory used by the process.
- Response Time - It represents the total time required to serve the request.

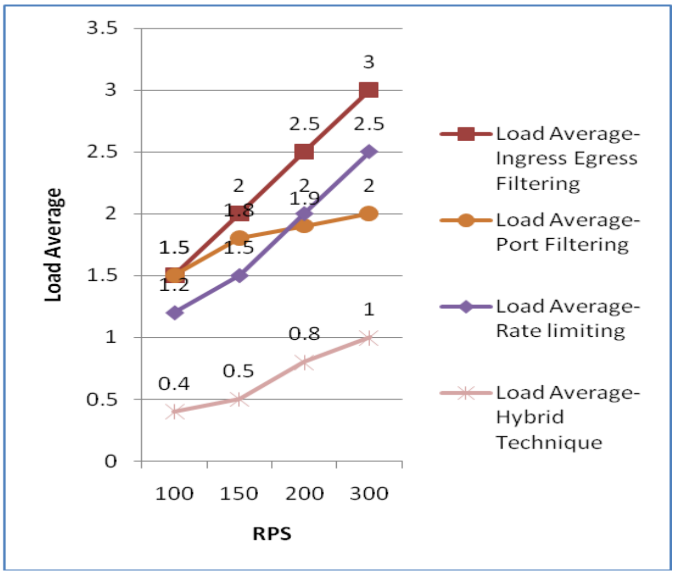

Chart-1. RPS to Load Average graph for different techniques

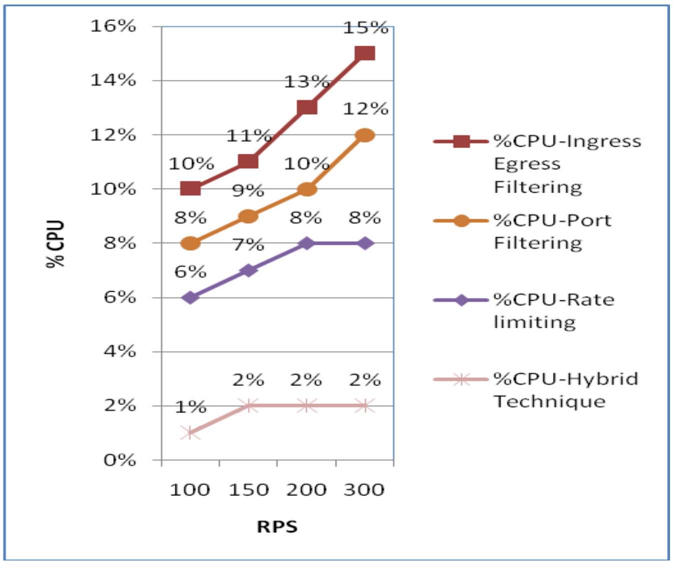

Chart-2: RPS to %CPU graph for different techniques

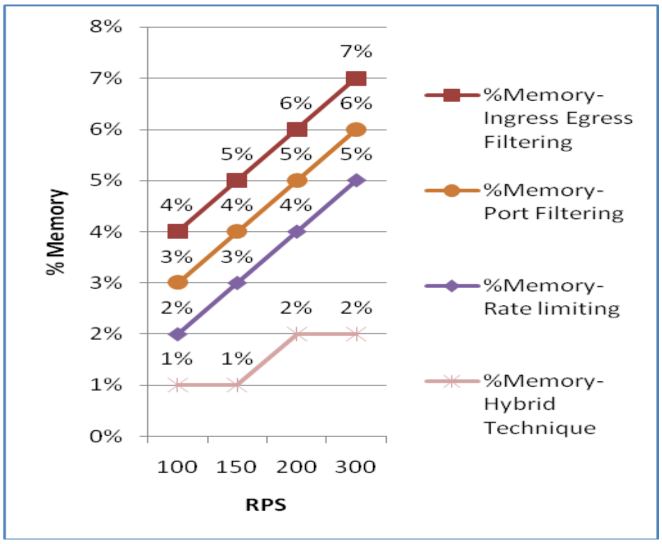

Chart-3: RPS to %Memory graph for different techniques

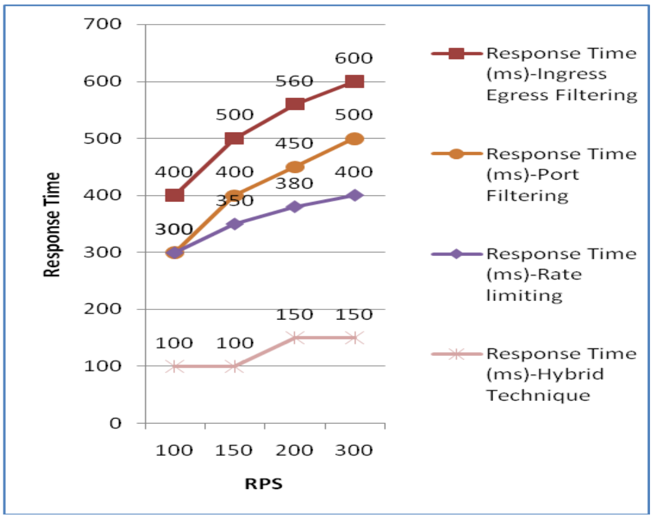

Chart-4. RPS to %Response Time for different techniques

Here, as we can see, different techniques like ingress-egress filtering, port filtering, rate limiting, and hybrid technique are compared with evaluation parameters like %CPU, %Memory, Load Average, Response time and we can see hybrid technique can effectively keeps the parameter in control keeping, cpu, memory utilization ,load average and response time low and better than all other techniques.

6. CONCLUSION

Here, as depicted in results, the parameters like %CPU, %Memory, Load Average and Response time are comparatively low in hybrid technique than any other techniques. Hence, we can conclude that our devised algorithm effectively defends and mitigates multilayered DDoS attacks and keeps the availability of the services least-affected and high. So, the devised technique effectively defends and mitigates both network and application layer attacks.

REFERENCES

[1] Dr. L. Visalatchi, PL. Yazhini, "The Survey DDoS Attack Prevention and Defense Technique" in International Journal of Innovative Science and Research Technology, Volume 5, Issue 2, February – 2020

[2] Inzimam Ul Hassan, Amandeep Kaur, "Literature Review on Prevention and Detection of DDoS Attack" in International Journal of Engineering and Techniques - Volume 4 Issue 2, Mar – Apr 2018

[3] Ahmed Bakr, A. A. Abd El-Aziz and Hesham A. Hefny, "A Survey on Mitigation Techniques against DDoS Attacks on Cloud Computing Architecture," in International Journal of Advanced Science and Technology, Vol. 28, No. 12, (2019), pp. 187-200.

[4] Sushmita Chakraborty, Praveen Kumar, Dr. Bhawna Sinha, "A STUDY ON DDOS ATTACKS, DANGER AND ITS PREVENTION", in IJRAR May 2019, Volume 6, Issue 2 www.ijrar.org (E-ISSN 2348-1269, P- ISSN 2349-5138)

[5] S. Dong, K. Abbas, and R. Jain,"A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments" in IEEE Access, Volume 7, pp. 80813-80828, 2019.

[6] Seth Djane Kotey, Eric Tutu Tchao and James Dzisi Gadze, "Review On Distributed Denial of Service Current Defense Schemes" in MDPI at 30 January 2019.

[7] T Mahjabin, Y Xiao, G Sun, "A survey of a distributed denial-of-service attack, prevention, and mitigation techniques", International Journal of Distributed Sensor Networks 2017, Vol. 13(12)

[8] Deepika Mahajan, Monika Sachdeva, "DDoS Attack Prevention and Mitigation Techniques - A Review", International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013

[9] Parneet Kaur, Manish Kumar & Abhinav Bhandari (2017), "A review of detection

approaches for distributed denial of service attacks, Systems Science & Control Engineering", 5:1, 301-320, DOI: 10.1080/21642583.2017.1331768..

[10] GulshanShrivastava and Kavita Sharma,"The Detection & Defense of DoS & DDoS Attack: A Technical Overview" Proceeding of ICC, 27-28 December 2010.

[11] Yaar, A., A. Perrig and D. Song, "Pi: A Path Identification Mechanism to Defend against DDoS attacks. Proceedings of Symposium on Security and Privacy", pp: 93-107, 2003.

[12] I. B. Mopari, et al., "Detection and defense against DDoS attack with IP spoofing," in Computing, Communication and Networking, 2008. ICCCn 2008. International Conference on, 2008, pp. 1-5.

[13] K. Lakshminarayanan, D. Adkins, A. Perrig, and I. Stoica. "Taming IP packet flooding attacks. SIGCOMM Comput. Commun. Rev.", 34(1):45–50, 2004.

[14] IT.V.S.Jeganathan, IIT. Arun Prakasam, "Secure the Cloud Computing Environment from Attackers using Intrusion Detection System", Vol. 2, Issue 2, Ver. 2 April - June 2014.

[15] Shaila R Ghanti, G.M. Naik, "Protection of server from syn flood attack", Volume 5, Issue 11, November (2014), pp. 37-46.

[16] P. Ferguson et. al., "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", Technical report, The Internet Society, 1998.

[17] Vern Paxson, Steve Bellovin, Sally Floyd and Ratul Mahajan, "Controlling high Bandwidth Aggregates in the Network" A Technical report 2002.

[18] H. Wang, C. Jin, and K. G. Shin, "Defense against Spoofed IP Traffic using HopCount Filtering", ACM Transactions on Networking. Vol. 15, pp. 40 – 53, 2007.

[19] H. Beitollahi and G. Deconinck, "Analysing Well-Known Countermeasures against Distributed Denial of Service Attacks" In Computer Communications, Elsevier, Vol. 35, issue 11, pp. 1312-1332, 2012.

[20] W. Eddy, "TCP SYN Flooding Attacks and Common Mitigations," RFC 4987, August 2007.

[21] Moti Geva, Amir Herzberg, and Yehoshua Gev," Bandwidth Distributed Denial of Service: Attacks and Defenses", Copublished by the IEEE Computer and Reliability Societies January/February 2014.

[22] Yongdong Wu, Zhigang Zhao, Feng Bao, and Robert H. Deng," Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 1, January 2015.

[23] Sunny Behal and Krishan Kumar, "Characterization and Comparison of DDoS Attack Tools and Traffic Generators - A Review". International Journal of Network Security,19(3):383–393, 2017.

[24] Protecting Shared Infrastructure. Best Practices for DDoS Protection and Mitigation on Google Cloud Platform.

https://cloud.google.com/files/GCPDDoSprotection-04122016.pdf, 2016.

[25] Kaspersky Labs. Global it security risks survey 2015. https://media.kaspersky.com/en/business-security/it-security-risks-survey-2015.pdf.

[26] Zargar ST, Joshi J and Tipper D. "A survey of defense mechanisms against distributed denial of service (DDoS) looding attacks. IEEE Commun Surv Tut 2013"; 15(4): 2046–2069.

[27] Ferguson P., Senie D. 2001, "Network ingress filtering: defeating Denial of Service attacks which employ IP source address spoofing. In RFC 2827".

[28] Peng T., Leckie C., and Ramamohanarao K. 2007, "Survey of Network Based Defense Mechanism Countering the DoS and DDoS Problems", Computer Journal of ACM Computing Surveys, vol. 39, Issue 1, pp. 123-128.

[29] "Ddos-attack-ex", Accessed on: Jan 24, 2021. [Online]. Available: https://upload.wikimedia.org/wikipedia/commons/9/93/Ddos-attack-ex.png

[30] Jan Engelhardt, Netfilter components, Feb. 28, 2014. Accessed on: Jan 24, 2021. [Online]. https://upload.wikimedia.org/wikipedia/commons/d/dd/Netfilter-components.svg

[31] I Putu Agus Eka Pratama, "TCP SYN Flood (DoS) Attack Prevention Using SPI Method on CSF: A PoC", Vol. 1, No. 2, December 2020, pp. 63~72, ISSN: 2722-7324, DOI: 10.25008/bcsee.v1i2.7

[32] Nipa Patani and Rajan Patel, "A Mechanism for Prevention of Flooding based DDoS Attack", International Journal of Computational Intelligence Research, ISSN 0973-1873 Volume 13, Number 1 (2017), pp. 101-111.

[33] Muhammad Tahir, Mingchu Li, Naeem Ayoub, Usman Shehzaib, Atif Wagan, "A Novel DDoS Floods Detection and Testing Approaches for Network Traffic based on Linux Techniques", (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 9, No. 2, 2018

[34] Bahaa Qasim M. AL-Musawi, "MITIGATING DoS/DDoS ATTACKS USING IPTABLES", International Journal of Engineering & Technology IJET-IJENS, 2012 Vol: 12 No: 03

[35] Vidya P N, Dr. Shrinivasa Naika, "SIMPLE TEXT BASED CAPTCHA FOR THE SECURITY IN WEB APPLICATIONS", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April- 2015, pg. 519-531.

[36] A.Saravanan, S.SathyaBama, Seifedine Kadry, Lakshmana Kumar Ramasamy, "A new framework to alleviate DDoS vulnerabilities in cloud computing", International Journal of Electrical and Computer Engineering (IJECE), Vol. 9, No. 5, October 2019, pp. 4163~4175.

[37] M. G. Mihalos, S. I. Nalmpantis and K. Ovaliadis, "Design and Implementation of Firewall Security Policies using Linux Iptables", Journal of Engineering Science and Technology Review 12 (1) (2019) 80 – 86.