Security against DDoS Attack – A Review

Jogin Joshi[#1], Jitendra Dhobi[#2], Dr. Dhaval Parikh[#3]

[1]*Scholar, Computer Engineering Department, GEC, Gandhinagar, India*
[2]*Associate Professor, Computer Engineering Department, GEC, Gandhinagar, India*
[3]*Professor & HOD, Computer Engineering Department, GEC, Gandhinagar, India*

---***---

Abstract – *DDoS stands for Distributed Denial of Service. This type of attacks affects availability of a service like diminishing performance or downtime of the service. Based on the protocol it affects, there are mainly two types of attacks network and application layer attacks. TCP, UDP Flooding, etc are examples of network layer attacks and HTTP attack is an example of application layer attack. There are various prevention and mitigation techniques like rate limiting, stateful packet inspection, ingress-egress filtering, CAPTCHA etc all works on countering some specific layer attacks. The paper outlines the major attacks and prevention defense techniques employed to counter them.*

Key Words: DDoS, Detection, Prevention, Mitigation, Flooding.

1. INTRODUCTION

Service availability is used to measure the how much time the service is able to run the intended function. It is very important for any service. DDoS (Distributed Denial of Service) is an attack where malicious request are sent with so overwhelming volume that it results in degradation or outage of the service. [3]

DDoS attacks are very harmful to individuals, service owners as well as businesses. Daily thousands of attacks happen all around the world and targets are ISPs, banks and other organizations majorly. [7]

2. OVERVIEW OF DDOS ATTACKS

2.1. DDoS Motives

The major motives behind DDoS attacks are as below:

1) Financial gains: Few attacks try to exploit the service to get some monetary gains out of it. [7]

2) Revenge: Personal, professional revenge is also an observed motive behind DDoS attacks where DDoS attacks are planned and executed to fulfill the revenge. [7]

3) Ideological differences: Sometimes due to ideological and political differences some attackers attack on particular service. [7]

4) Intellectual reasons: The attackers sometimes attack to prove their potential as an attacker. It is one of the psychological reasons behind the attack. [7]

5) Cyberwarfare: Sometimes countries or terrorists use DDoS attacks to adversely affect some other country or organization. [7]

2.2. Types of DDoS Attack

DDoS attacks are majorly of below two types:

1) Network/transport layer attacks: This type of attacks operates on network or transport layers. Flooding attacks like SYN, UDP, ICMP etc are examples of it.[3][6]

2) Application layer attacks: This type of attacks operates on application layer of the service. HTTP, DNS attacks are examples of this attacks. [3][6]

2.3. Examples of DDoS Attacks

1) Smurf Attack: Here attacker uses entire network to generate very high volume of traffic to down the victim service. [6]

2) HTTP Flood Attack: In this type of attack overwhelming HTTP requests are generated to the victim much such that high computing resources are wasted which makes the service unavailable. [7]

3) UDP Flood Attack: As UDP services listens on particular port to serve the requests coming to that port. Here due to malicious requests to the port server continuously replies with “ICMP Host Unreachable” packet. It leads to high wastage of resources and makes the service unresponsive. [7]

4) SYN Flood Attack: Three way handshaking is a mechanism where SYN, SYN-ACK and ACK packets packet sequence is followed to make a TCP connection. In SYN flooding, spoofed SYN requests are sent to victim service, service replies with SYN-ACK and as the requests are spoofed no ACK comes. It leads to half-open connection and in a short time leads to connection exhaustion and unavailability of service. [6][7]

3. LITERATURE REVIEW

(I Putu Agus Eka Pratama)[31] In this paper TCP SYN flood is discussed which is a type of Denial of Service (DoS) attack. Here, excessive SYN requests are sent and due to spoofing, it leads to exhaustion of connections. Here SPI (Stateful Packet

Inspection) method is used to check the packets as it passes and drop them if they exceed some predefined rate.

(Nipa Patani and Rajan Patel)[32] This paper discusses prevention of flooding attacks which are type of DdoS attacks. They are more harful than any other attacks. Here, CAPTCH (Completely Automated Public Turing test to tell Computers and Human Apart) is employed to defend application layer attacks.

(Vidya P N, Dr. Shrinivasa Naika)[35] This paper is focused on text based CAPTCHA approaches which can effectively distinguish between bots and human by representing and taking inputs of annotated text CAPTCHA. It can restrict automated attacks by making mandatory CAPTCHA authentication before web application usage.

(Dr. L. Visalatchi, PL. Yazhini)[1] In this paper various attack types like UDP flood, SYN Flood, ping of death etc are discussed along with defense techniques like rate limiting, ingress-egress filtering etc.

(Inzimam Ul Hassan, Amandeep Kaur)[2] This paper shows various prevention techniques like ingress-egress filtering, rate limiting, CAPTCHA techniques, Puzzle technique which can be employed against DDoS attacks.

(Sushmita Chakraborty, Praveen Kumar, Dr. Bhawna Sinha)[4] In this paper, various terms related to DDoS attacks are discussed especially in ISP industry context. It also shows how it affects various industry types.

(Tasnuva Mahjabin, Yang Xiao, Guang Sun and Wangdong Jiang)[7] This paper elaborates various DDoS attacks and mitigation approaches. It also studies various motives behind the attack like economic gain, hostility, warfare etc. It details attack types like flooding, amplification attacks etc.

(Deepika Mahajan, Monika Sachdeva)[8] The paper describes study about various prevention techniques and defense approaches like ingress-egress filtering, rate limiting, history based filtering etc.

4. MITIGATION AND DEFENSE TECHNIQUES

4.1. Rate Limiting

Rate limiting is a technique to limit the rate of the packets with the predefined conditions like source, destination, port or any combination. All the packets that exceed the rate are dropped. [1]

4.2. Ingress and Egress Filtering

Ingress and Egress filtering is used to do inbound and outbound filtering which drops all the packets from unknown ports in input and output interface respectively. [1]

4.3. CAPTCHA based defense

CAPTCHA stands for Completely Automated Public Turing Test to tell Computers and Humans Apart which is used to differentiate between human and boats. Based on that the boat requests are dropped and such malicious requests become unable to hamper the service. It is used to defend application layer DDoS attacks. [2]

4.4. Software puzzle based problem

This is approach similar to CAPTCHA being puzzle as a way to differentiate between human and bots. Only human can solve the puzzle and able to proceed further. It can be used to defend application layer DDoS attacks. [2]

4.4. Blacklisting and Whitelisting

In this technique, blacklisting and whitelisting of ipaddresses are maintained. When a ipaddress is encountered, it is tested for human or bot. If it is a bot, it gets blacklisted or else it is whitelisted. [3]

5. CONCLUSION

There are multiple layers on which DDoS attacks affects different systems like transport layer attacks i.e. TCP, UDP, ICMP or application layer like HTTP etc. We have different defense and mitigation techniques as well like rate limiting, ingress-egress filtering, CAPTCHA based defense but those techniques works on individual attack and they doesn't seem working cohesive and integrative way. So, we need an integrated and cohesive approach to defend and mitigate multilayered DDoS attack.

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) flooding 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.

[38] "What Is a Distributed Denial-of-Service (DDoS) Attack?", Accessed on: Jan 24, 2021. [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[39] "Rate Limiting", Accessed on: Jan 24, 2021. [Online]. Available: https://www.cloudflare.com/en-in/rate-limiting/

[40] "Understanding How Firewall Filters Control Packet Flows", Accessed on: Jan 24, 2021. [Online]. Available: https://www.juniper.net/documentation/en_US/junos/topics/concept/firewall-filter-qfx-series-packet-flow-understanding.html

[41] "Whitelisting versus Blacklisting", Accessed on: Jan 24, 2021. [Online]. Available:

https://www.chorus.co/resources/news/whitelisting-versus-blacklisting-anti-virus-software

[42] "CAPTCHA", Accessed on: Jan 24, 2021. [Online]. Available: https://www.flickr.com/photos/engineroomblog/4042869841

[43] Laura Entis, Google Says R.I.P. to CAPTCHA (Sort Of), Dec. 4, 2014. Accessed on: Jan 24, 2021. [Online]. Available: https://www.entrepreneur.com/article/240478

[44] "Netfilter", Accessed on: Dec. 1, 2020. [Online]. Available: https://whisperlab.org/introduction-to-hacking/talks/netfilter

[45] "Iptables", Accessed on: Jan 24, 2021. [Online]. Available: https://www.dbsysnet.com/wp-content/uploads/2015/12/iptables.png

[46] "Iptables", Accessed on: Dec. 1, 2020. [Online]. Available: http://fleming0.flemingc.on.ca/~chbaker/COMP232-FW-IDS/COMP232-01a-iptables.pdf

[47] "User specified chains", Accessed on: Jan 24, 2021, 2020. [Online]. Available: https://wm-help.net/lib/b/book/1259475082/78

[48] "How does a packet traverse from one local process to another local process in the following iptables graph? - Server Fault", Accessed on: Jan 24, 2021, 2020. [Online]. Available: https://serverfault.com/questions/342205/how-does-a-packet-traverse-from-one-local-process-to-another-local-process-in-th

[49] "DDoS attacks in Q1 2020", May 6, 2020. Accessed on: Jan 24, 2021, 2020. https://securelist.com/ddos-attacks-in-q1-2020/96837/

[50] "DDoS attacks in Q2 2020", Aug. 10, 2020. Accessed on: Jan 24, 2021, 2020. https://securelist.com/ddos-attacks-in-q2-2020/98077/