International Journal of Intelligent Computing and Technology
ISSN: 2457-0249 (Online)
Website: https://www.ijict.com Jan (2022) - Vol.5, Iss.2 Pages:55-62

A STUDY ON DISTRIBUTED DENIAL OF SERVICE ATTACKS

Sulochana V[1], Kamali P[2], Kulandai Priya V[3]
[1,2]BSc Computer Science, [3]Programmer,
PG Department of computer science, Holy Cross College, Trichy, Tamilnadu

Article History- Received: June 2021; Published: Jan 2022

Abstract

Distributed Denial of Service attack is one of the web-based service's most strong and overwhelming challenges. These DDOS attacks can't be avoided in advance, and once in position, they overwhelm the target with immense volume of traffic and make him unable to interact normally or completely crash it. If the identification of flooding attacks is delayed, nothing much can be done except to propose isolate the victim manually and fix the problem. In this paper, we HADEC, a live DDOS Detection system built on Hadoop to solve efficient analysis of flood attacks by using MapReduce and HDFS.

Keywords: *DDoS, Flooding attacks, DDoS Detection, Hadoop, MapReduce*

1. INTRODUCTION

DOS flooding attacks are one of the major threats to sensitive IT infrastructure, ranging from the simplest business network to complex corporate networks. DDOS has hit major corporations and Internet infrastructure, resulting in significant revenue losses. Big DDOS flooding attacks and the Mastercard, Post Finance, and Visa websites were brought down.

Study of recent attacks shows that, with little effort, the next generation of attack tools would be able to implement DDoS attacks that are a thousand times stronger than those we see today. One of the main concerns is that DDoS attacks are extremely simple with websites such as Booster or Stressers providing DDoS as a service.

The exponential rise in the amount of Internet traffic and the complexity of DDoS attacks have presented serious challenges to the robust and accurate analysis of the DDoS attacks. For example, in order to detect anomalies, two of the most popular open-source intrusion detection systems (IDS), Snort and Bro, maintain per flow state. The real motivation behind this study is to use modern distributed architectures that can run-on low-cost commodity hardware to test the efficacy of scalable defenses against DDoS flooding attacks. The real motivation behind this study is to use modern distributed architectures that can run-on low-cost commodity hardware to test the efficacy of scalable defenses against DDoS flooding attacks.

HADEC consists of two main components, a server for collection and a server for detection. Live DDoS begins with the capture by the capturing server of live network traffic. The capturing server then processes the traffic captured to produce log file and transfer it for further processing to the detection system. A Hadoop cluster is handled by the detection server, and when log files are provided, DDoS detection based on MapReduce begins joining jobs on the cluster nodes

2. BACKGROUND STUDY

Sufian Hameed et.al. detaily explained the DDoS attacks cannot be avoided in advance, and once there, they overwhelm the target with an immense volume of traffic and render him unable to interact normally or completely crash it. A hadoop-based live DDoS detection framework to effectively address flood assault an analysis using MapReduce HDFS harnessing. MapReduce, a counter-based DDoS detection algorithm implemented for four major flooding attacks (TCPSYN, HTTP GET, UDP, and ICMP), consisting of mapping and reduction of function. Ashwini Khadke et.al. Described the paper of Distributed Denial of Service (DDoS) attacks aim to exhaust various victim hosts ' resources, thus preventing the legitimate use of their computational capabilities. DDos attacks are often launched ads by organized crime, hacktivists, or other (un)usual suspects, making this type of cyber crime a major concern in cloud computing for many organizations around the world performance plays a significant role. Jiang et.al. examined the impacts of DDoS attacks on the application layer including existing attacks on HTTP/1.1 and the new attacks proposed by us against HTTP/2.0.

Shin Dong et.al. defined the Researchers and industry have recently adopted the software-defined networks (SDNs) and cloud computing. Nevertheless, the widespread adoption of these novel networking paradigms has been hindered by threats to protection. Advances in computing technology have also helped attackers increase attacks, such as the development of Denial of Service (DoS) attacks on distributed DoS (DDoS) attacks that traditional firewalls seldom recognize.

Antry Putra et.al. presented the Current network development has entered the era of Software Defined Networking (SND) that offers centralized network control and programmability by decoupling the network control and data plane that brings us a dynamic, cost-effective, manageable and agile platform. On the downside, this centralized platform can present new security challenges such as DDoS attacks on a central controller that could compromise the entire network. This paper presents SDN security challenges and provides several approaches for mitigating DDoS attacks from different sources.

3. METHODOLOGY

You need to prepare and schedule your system for a DDoS attack. You need to track the generation of warnings and diagnose an active DDoS attack quickly. The next move is to quickly shut down the attack without impacting the users. Using your next-gen firewall, you can block IP addresses or close in bound traffic to the targeted system and fail to backup.You can implement other response plans, makesure you have one.

3.1 COMMON TYPES OF DDoS ATTACKS

There are numerous ways in which attackers can sustain a DDoS attack. Here are some of the best known.

A) Application Layer Attacks B) Protocol Attacks C) Volumetric Attacks

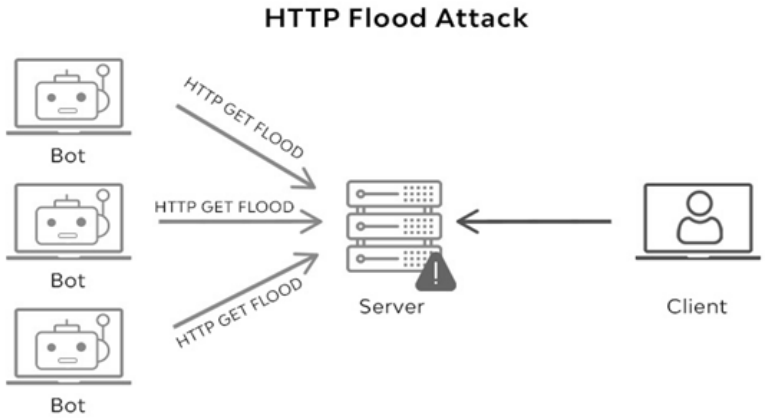

Fig 1 HTTP Flood Attack

A) APPLICATION LAYER ATTACK

Application layer DDoS attacks attempt to drain target resources and interfere with the website or service of the target. Attackers load bots with a complicated request that taxes the destination server and it attempts to respond. An application can allow access to the database or large downloads. If the target receives several million of those requests in a short time, it can get overwhelmed very quickly and either slow to crawl to lock it up.

For example, an HTTP Flood attack is an application layer attack that targets a target web server and uses a lot of quickly. HTTP requests to access the file. Think of it as pressing the quick-fire button on your game controller. Such traffic from thousands of computers would flood the web server easily at once [9].

B) Protocol Attack

DDoS protocol attacks target the target device networking layer. Their aim is to overpower the core networking services table spaces, firewall, or load balancer that forward requests to the target.

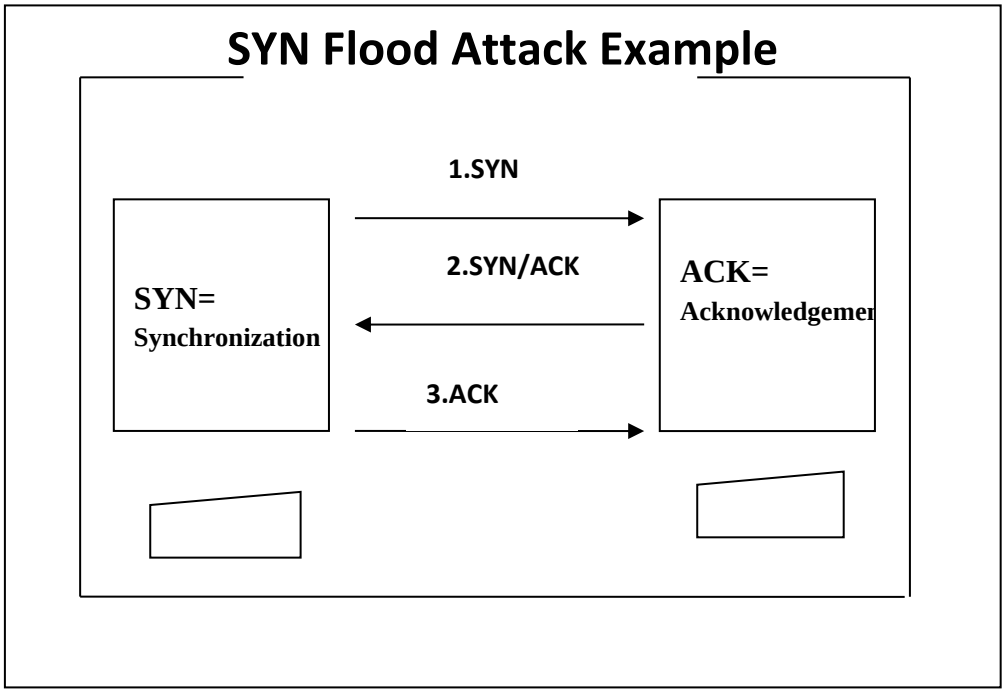

Fig 2 Protocol Attack

Network services generally operate a first-in, first-out (FIFO) queue. The first request is received, the computer processes the request, and then the next request is received in the queue, etc. There is now a limited number of sports on this queue, and in a DDoS attack the list could become so large that the machine does not have the resources to handle the first request.

A flood attack from SYN is a particular attack from the protocol. A 3-way handshake is required in the regular TCP / IP network transaction. These are the first component of the SYN, which is a request of some kind, the ACK is the answer from the target, and the SYN-ACK is the original request saying "thank you, I have received the information I asked for." The attackers create SYN packets with IP address in a SYN flood attack. The target then sends an ACK to a dummy address that never responds, and then sits there and waits for all those timely responses, which in turn exhausts the resources to handle all those fake transactions.

C) Volumetric Attacks

The purpose of a volumetric attack is to use the botnet to produce a large amount of traffic and to block the target's work. Think of it as an HTTP Flood attack, but with a part of exponential response.

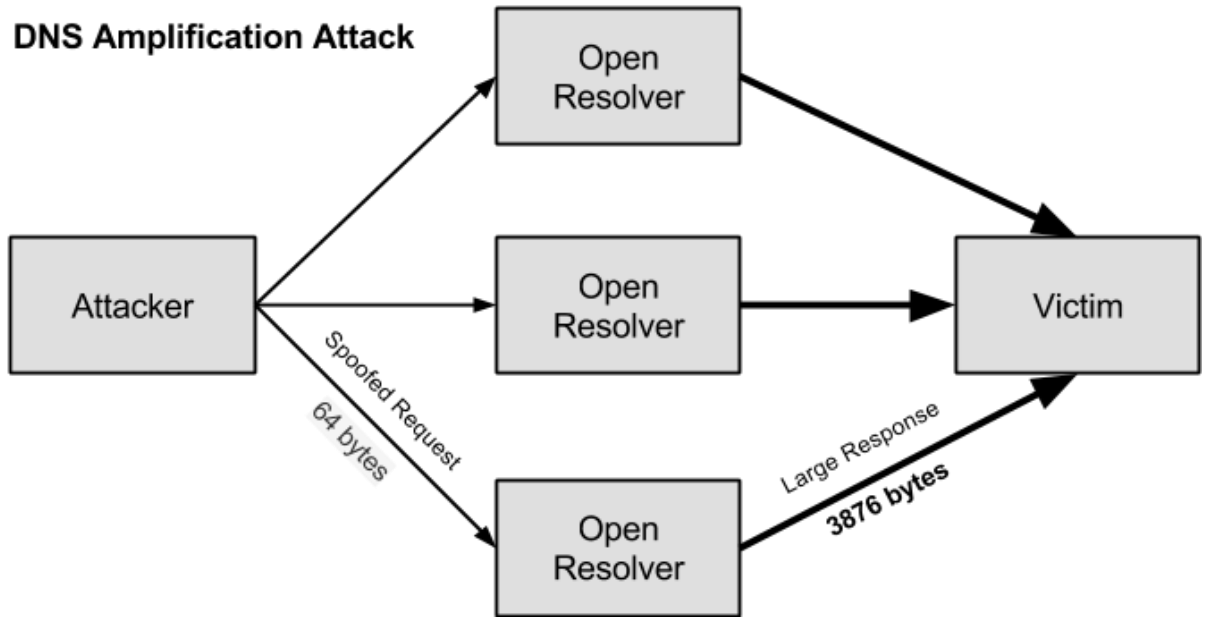

Fig 3 Volumetric Attack

For instance, if you and 20 of your friends dropped the same pizza place and ordered 50 pieces at the same time, the pizza shop wouldn't be able to meet those requests.

We are asking for something from the target that will greatly increase the answer size and the volume of traffic will burst and block the server.

Amplification of DNS is a sort of volumetric attack. In this case, the DNS server is attacked directly and a large amount of data is requested from the DNS server that can bring that DNS server to name resolution services.

3.2 Category

DDoS flooding attacks can be divided into two groups Depending on the target protocol level: Network / Transport level attacks (UDP flooding, ICMP flooding, DNS flooding, TCP SY flooding, etc.) and application level attacks (HTTP GET / POST request). The methods of defense against DDoS flooding attacks at the network or transport level fell approximately into four categories: A) Source-based B) Destination-based C) Network-based and D) Hybrid (distributed)

Application level DDoS flooding protection mechanisms are divided into two main categories: destination based and hybrid (distributed). Since application traffic is not accessible at layers 2 and 3, the application level DDoS has no network based defense mechanism.

A) Source-Based

The detection and response is deployed at the source hosts in the source based defense mechanism in an attempt to mitigate the attack before wasting lots of resources. With this approach, consistency is a major concern because it is difficult to differentiate legitimate and DDoS attack traffic from sources of low traffic volume. In addition, the source ISP has poor incentive for Deployment due to higher community service costs.

B) Destination-Based

In this case, the mechanisms of detection and response are deployed on the host destination. Access to aggregate traffic near the destination hosts makes DDoS attack detection faster and cheaper than other methods with high accuracy. On the downside, mechanisms based on destination can not preempt an attack response before it reaches the target and wastes resources on the victim's routes.

C) Network-Based

Detection and response was implemented in intermediate networks with network-based approach. The idea behind this approach is to filter the intermediate network attack traffic as close as possible to the source.

Network-based DDoS defense involves high overhead storage and processing on routers, and precise detection of attacks is also difficult due to the lack of sufficient aggregate traffic for victims.

D) Hybrid (Distributed)

In the hybrid approach, there is communication between different components of the network along the path of attack and mechanisms of detection and response are deployed at different locations.

Destination hosts and intermediate networks typically deploy detection mechanisms, and response usually takes place near sources and upstream routers. Hybrid approach is more effective against DDoS attacks, but it takes more resources at different levels to deal with DDoS attacks due to distributed design. Another limiting factor in the smooth deployment of hybrid-based DDoS defenses is the complexity and overhead due to the coordination and communication between distributed components.

3.3 HADOOP DDoS Detection Framework

This section offers insights into how our proposed system works. The Hadoop-based live DDoS detection framework (HADEC) comprise of four major phases. A. Network traffic capturing and log generation B. Log transfer C. DDoS detection. D. Result notification.

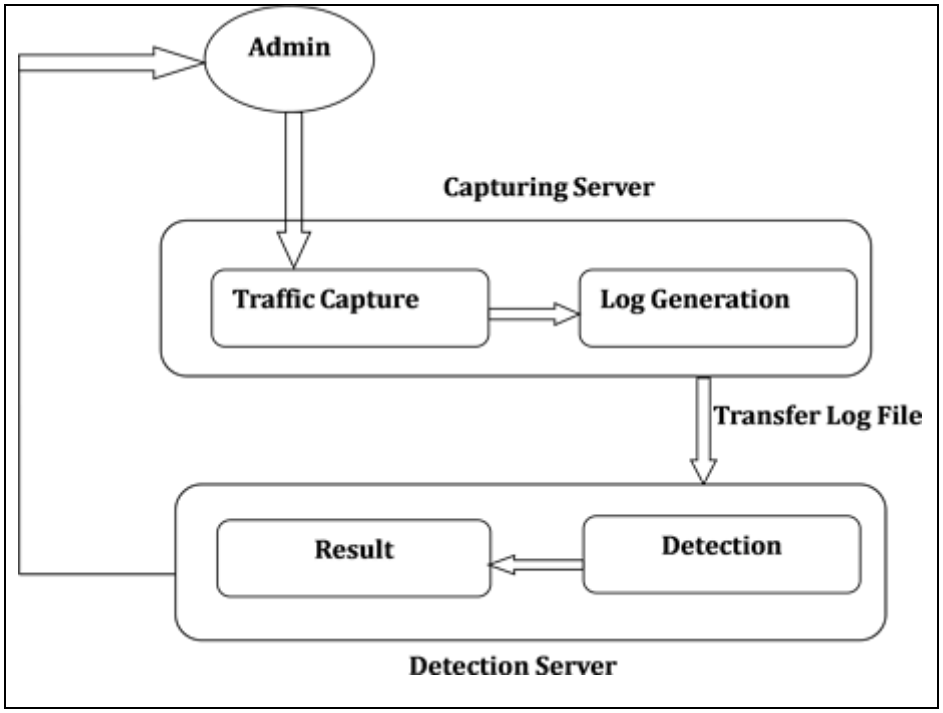

Fig 4 DDoS detection framework

Traffic Capturing and Log Generation

Detection of Live DDoS begins with network traffic capture. HADEC offers a web interface that allows the admin to set the necessary parameters to the capture server. These parameters are the size of the file, the number of files to be captured before the detection phase starts, and the path to save the captured file. Once the configuration is done for the admin, The Traffic

Handler sends the Echo Class property file (a java utility to generate logs) and starts capturing live network traffic.

Options, malicious actors may pay a nominal fee to "rent" a botnet of infected Computers to launch a DDoS attack against their preferred target. Attackers Targeted both Wikipedia and Classic Warcraft World with DDoS attacks in September 2019. There is no indication at the moment that these attacks are new Technology, but they remain tuned for any updates.

4. Conclusion

It has been demonstrated that DDoS attacks are an effective way on disrupt web services. DDoS attack will remain a constant threat to large and small organizations amid advancements in mitigation and prevention techniques. A good starting point is a privacy and security mentality, starting with encrypted email and pursuing good online privacy/security processes. It reduces the chance that your machines will transform into a bot that will lead to DDoS attacks. We take security on infrastructure as one of the most secure and private email suites and strive to improve the security of our service in every way possible.

REFERENCES

1. Hameed, S., Ali, U.: Efficacy of live DDoS detection with Hadoop. In: IEEE/IFIP Network operations and Management symposium (NOMS), PP.488-494 IEEE (2016).
2. Ashwini Khadke, Mangala Madankar, Manish Motghare: Review on Mitigation of Distributed Denial of Service (DDoS) Attack, IEEE 2016.
3. Andry Putra Fajar, Tito Waluyo Purboyo: A Survey Paper of DDoS attack in Software Defined Networking (SDN), 476-482
4. Jiang, M., Wang, c., Luo, X., Miu, M. T., & Chen, T. (2017). Characterizing the impacts of application layer DDoS attacks. In 2017 IEEE International Conference on Web Services (ICWS), 500-507, 2017.
5. Narasimha Mallikarjunan, K., Muthupriya, K., & Mercy Shalinie, S. (2016). A survey of distributed denial of service attack. In 2016 10th International Conference on Intelligent Systems and Control (ISCO)
6. Rama Krishna, C., Krishan Kumar (2019). Apache Hadoop Based Distributed Denial of Service Detection Framework. In 2019 IEEE Conference Paper.
7. Shi Dong, Khushnood Abbas, Raj Jain. A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access7, 80813-80828,2019.
8. Singh, k., Singh, p., Kumar, k: Application Layer HTTP-GET flood DDoS attacks: research landscape and challenges. Comput. Secur.65, 344-372 (2017).
9. Subhi R.M. Zeebaree, Karzan H. Sharif, Roshna Muhamad M. Amin: Application Layer DDoS Attacks Defence Techniques: A review, IEEE 2019
10. Wang, Y., Liu, L., Si, C., & Sun, B. (2017). A novel approach for countering application layer DDoS attacks. In 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAB).

How to cite this article:
Sulochana V, Kamali P, Kulandai Priya V, "A Study on Distributed Denial of Service Attacks", International Journal of Intelligent Computing and Technology (IJICT), Vol.5, Iss.2, pp.55-62, 2022