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 send 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 many 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

![Component flow for proposed system](image)

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.

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](chart1.png)

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

![Chart-2](chart2.png)

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

![Chart-3](chart3.png)

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

![Chart-4](chart4.png)

**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


