A Survey on Distributed Denial of Service and its Implications

Soumee Maschatak
Department of Computer Science & Engineering East West Institute of Technology
Bengaluru, India

Dhanraj DS
Department of Computer Science & Engineering East West Institute of Technology
Bengaluru, India

Abstract:- With the increased availability of the internet and the increased dependency of the people on the internet, cyber-attacks have become more prevalent. DDoS is one such of a cyber-attack. DDoS is a kind of DoS attack which can have many sources and it's difficult to stop or prevent the attack. In this paper, we are going to present a detailed description about the DoS attack, its types, its effects and its prevention mechanisms.

Keywords:- *Denial-of-Service, Distributed Denial- of-Service attack,*

I. INTRODUCTION

A Denial-of-Service (DoS) is a type of attack in which the legitimate users are devoid of using their own machine or network often leading to the shutdown of the machine or the network. Dos attack is often accomplished by flooding the target machine with traffic or irrelevant information which results in triggering the machine to crash. In either of the cases, the legitimate users are deprived of the machine and the resources they expect to use.

Victims of DoS attack are mainly the websites and the servers of the highly profiled organizations such as Medias, governmental sectors, banking and many such others. Though DoS attack does not result in any loss or theft of information, it can result in significant delay in the transmission of the important information and also prevent the legitimate users from reaching the rightful information.

A Denial-of-Service attack is used to keep the network resources engaged or tied up so that the users who need to have access to the resources, are never allowed to do so. Many major and big companies have been the victims of such attacks. A DoS attack can be engineered from any location around the world, thus, making it extremely difficult to reach the source or the people responsible for the attack.

The main aim of the DoS attack is to overfill the request queue of the target website, server or the network. Multiple attacks to the same target can be categorized by the similarity in the type of the attack.

There are two different methods of DoS attacks: flood attacks and crash attacks.

Flood attacks occur when too many requests are received from the server to the system, causing it to buffer and slow down the machine eventually leading to its shutdown. The following are the most popular flood attacks:

- **Buffer overflow attacks** – It is the most popular kind of flood attack. Here the system receives more traffic than it is programmed to handle. It floods the network addresses byan excessive amount of information causing the system to lag or slow down.
- **ICMP flood or Smurf** – It takes advantage of the misconfigured network devices by sending spoofed data packets to every computer connected to the targeted network. The network then amplifies the traffic. This type of attack is more sensitive as it does not attack any specific target machine, instead it attacks all the computers connected to that network. The effect of this is slowing down the network to a point where it is impossible to use it.
- **SYN flood** – It is a type of flood attack in which the user sends a request to connect to the server but it never completes the handshake. The user goes on flooding the server with the connection requests resulting in flooding of the requests at the server end. It continues until all the open ports are saturated with the requests resulting in denial of the connection request from legitimate users.
- **Teardrop -** this type of flood attacks uses large data packets. The transmission control protocols or the TCP/IP allows the transmission of the packets by fragmenting it into small packets which are assembled at the receiving end. The attacker manipulates the fragments so that they overlap each other. The overlapping of the packets prevents the reassembling of the packets at the receiving end.
- Other DoS attacks can be the type of attack in which the attacker takes advantage of the vulnerability of the targeted system or servers causing the services of the targeted system to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the system, so that it can't be accessed or used.

Crash attacks occur with very less frequency where the cybercriminals already has knowledge about the flaws of the existing system and transmit bugs in order to exploit the existing flaws of the targeted system. The results of the crash attack is to crash the system by causing it to slowdown initially. Both the crash attacks and flooding attacks are used to prevent the legitimate users from accessing the available online services such as bank accounts, websites, gaming sites, and email.

II. THE WORKING OF THE DoS ATTACK

A DoS attack is not depended on the installation of any special program in the system, unlike a virus or a malware. Instead it takes advantage of the inherent vulnerability of the communication capacity of the computer networks.

Here's an example. Suppose you wish to visit an e-commerce site in order to shop for a gift. Your computer sends a small packet of information to the website. The packet works as a "hello" – basically, your computer says, "Hi, I'd like to visit you, please let me in."

When the server receives your computer's message, it sends a short one back, saying in a sense, "OK, are you real?" Your computer responds — "Yes!" — and communication is established.

The homepage of the concerned website pops up on the screen and allows the user to explore the site. Meanwhile the computer and the server keeps on communicating as the user continues online shopping.

In DoS attack, the computer is made to send not one but thousands of requests to the server. The server which cannot distinguish between the fake and the original requests, sends back its usual response, waiting for up to a minute to hear each replies. When it does not get any replies, the computer shuts down the connection. The attacker keeps on repeating the process by sending a fresh batch of fake requests, until the server is no longer capable of serving any more requests.

➢ *Another types of attack: DDoS*

DDoS stands for Distributed Denial-of-Service. DDoS is a special type of DoS attack in which the victim is attacked from more than one sources. It is an evolution in the attack types of DoS since 2000. A few reasons why DDoS has gained popularity over time in the history of cyber-attacks.

The attack uses large number of compromised computers and other electronic devices which is used to force down the functioning of the targeted websites, server and network. The electronic devices that can be used for attacking can be webcams, smart televisions and many electronic mobile devices.

Security vulnerabilities in Internet-of-Things devices makes it easy for the cyber-criminals to launch the DoS attack on the victim.

A DoS attack in contrast to DDoS attack, uses a single computer to launch attack against the victim and hence can easily be identified and taken action against.

➢ *Some significant DoS attacks*

Historically, DoS attacks typically takes advantage or exploits the security vulnerabilities of the servers, the networks and the websites. These attacks have become more prevalent with the introduction of DDoS attacks as DDoS attacks are difficult to identify and stop. In reality, most DoS attacks can also be turned into DDoS attacks.

A few common historic DoS attacks include:

Smurf attack - Here the attacker floods the target machine by sending spoofed data packets by taking advantage of the vulnerability of the network.

Ping flood - This attack is based on the ICMP packets. This occurs by flooding the target machine with more number of pings than it can handle, which ultimately leads to DoS attack.

Ping of Death - A ping of death attack involves sending a malformed packet to a targeted machine, resulting in deleterious behavior such as system crashes.

➢ *Experiencing a DoS attack*

Some characteristics indicate that the computer is experiencing a DoS attack. The characteristics are the following –

- A slow performing computer and a slow network performance such as long loading time of the websites or files
- Inability to load the full website
- All the devices of the same network connectivity experiencing a sudden network loss connectivity.

➢ *DoS attack tools*

Some of the tools that can be used for performing DoS attacks are the following **-**

Nemesy– It is a windows tool which is used to generate random packets. It can be most likely detected as a virus, if an antivirus is installed in the computer due to the nature of the program.

- **Land and LaTierra**– this tool can be used for IP spoofing and opening TCP connections
- **Blast**– this tool can be used to blast the network with random connection request
- **Panther-** this tool can be used to flood a victim's network with UDP packets.

Botnets– Botnets are compromised computers of a network which can be used to launch distributed denial of service attack on the victims.

III. DISTRIBUTED DENIAL-OF-SERVICE ATTACK

A distributed denial-of-service attack occurs when the victim is targeted from multiple machines at the same time from different locations. The attackers mainly leverage the use of botnets to carry out the attack. The attackers take advantage of security vulnerability or weakness of the open ports to carry on the attack. It does not led to loss or theft of information, but it leads to the slowdown of the system leading to its complete shutdown. It is difficult to stop the DDoS attack as the attacker can be placed at any part of the world and also, the attackers are multiple at a time.

A distributed denial-of-service (DDoS) attack is a nefarious attempt to disrupt legitimate traffic of a targeted server, service or network by overwhelming or flooding the target or its surrounding infrastructure with Internet traffic. DDoS attacks achieves it effectiveness by utilizing multiple computers from different locations to target the victim server, network or the websites. The victim machines can also include IoT devices. A DDoS attack is like a traffic jam blocking the highway and preventing the normal traffic to reach its destination.

Botnets are one of the mechanism used to carry out the DDoS attack. Botnets consists of compromised devices which can be rented out to potential attackers. They are a useful instrument for the unskilled people to launch the DDoS attack.

DDoS increases the number of requests sent to the server exponentially, thereby increasing the attack power. It also increases the difficulty to identify the attacker machines as the attacker is multiple, located at different parts of the country.

With the increased popularity and demand for IoT devices, the DDoS attack has also increased in magnitude as the IoT devices are always connected to the internet. IoT devices often used default passwords which are usually very easy to crack and also the security of the IoT devices is quite vulnerable to hack. Intrusion into an IoT devices often goes unnoticed and hence it becomes easy for the attacker to conduct a high-scale attack without the knowledge of the owner of the device.

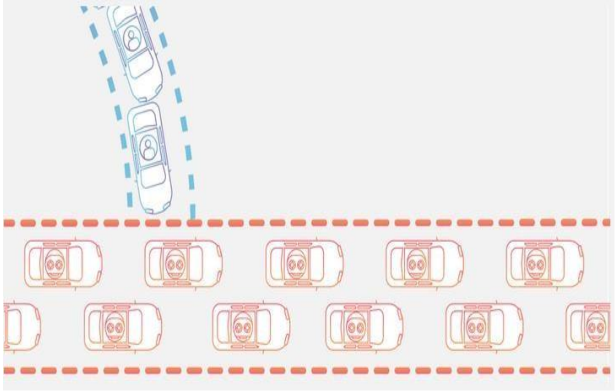

Fig 1:- Example of a DDoS attack

IV. DIFFERENCE BETWEEN A DDOS ATTACK AND A DOS ATTACK

The distinguishing difference between DDoS and DoS is the number of connections utilized in the attack.

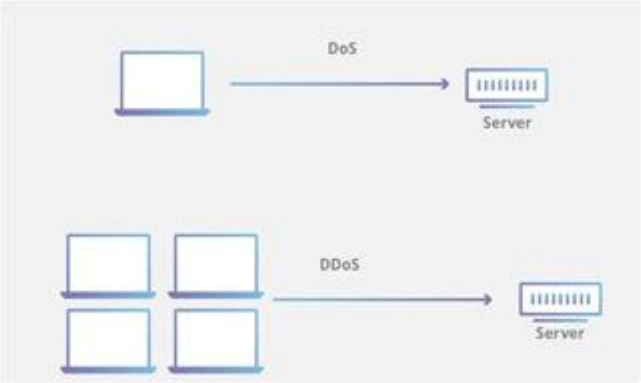

Fig 2:- A pictorial representation of the DoS and DDoS attack

DoS attack uses a single connection to attack the victim computer, server, network or the website. Whereas the DDoS attack takes place from multiple sources simultaneously, usually with the use of botnet. DoS attack is easy to identify as it is from a single source and often easy to control. But prevention of DDoS is not easy as it occurs from multiple sources. Often the source is spread across the world.

- *How does a DDoS attack work?*

A DDoS attack requires the attacker to take control of the network via which the machines to be attacked are connected. In this way, the attacker will have complete control over the network of the victim machines. The attacker can then use certain malware or the botnets to flood the victim machine with connection requests which will eventually lead to the shutdown of the victimized machine.

Once the botnet have been established, the attacker can start launching attacks by sending updated instructions to the victim machine via remote control. Each bot will then target the IP address of the victim by sending requests to the target and over flooding the target with the requests. This results in a denial of service to the legitimate requests. Separating the legitimate requests from the fake requests can be difficult as the fake requests has the same characteristics as the legitimate requests.

➢ *Common types of DDoS attacks*

DDoS attack can be different in different layers of the OSI model. In order to understand the different OSI layer attacks, let us first have a look into the different layers of the OSI model with the help of the diagram given below

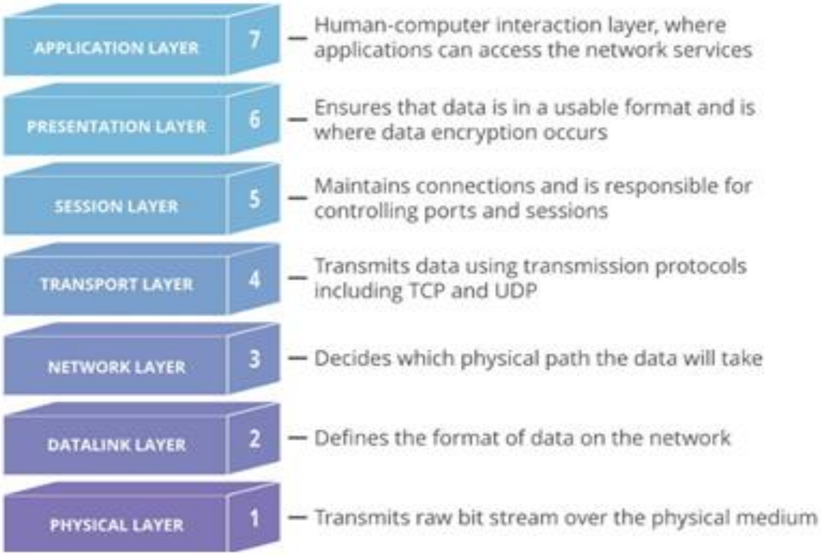
APPLICATION LAYER
7
Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
Decides which physical path the data will take
DATALINK LAYER
2
Defines the format of data on the network
PHYSICAL LAYER
1
Transmits raw bit stream over the physical medium

Fig 3:- OSI model

The DDoS attack for different layers can vary by attacking the different components of the machine at different layers. The DDoS attacks can be divided into three different categories. An attacker may make use one or multiple different attack vectors, or cycle attack vectors potentially based on counter measures taken by the target.

V. APPLICATION LAYER ATTACK

The goal of this attack is to exhaust the resources of the target. Also known as the 7th layer attack as the application layer is the topmost or the seventh layer of the OSI model. These attacks are used to target the layer where the web pages are generated on the server and the HTTP requests are handled. Application layer DDoS attack is difficult to mark as malicious and hence difficult to defend the traffic.

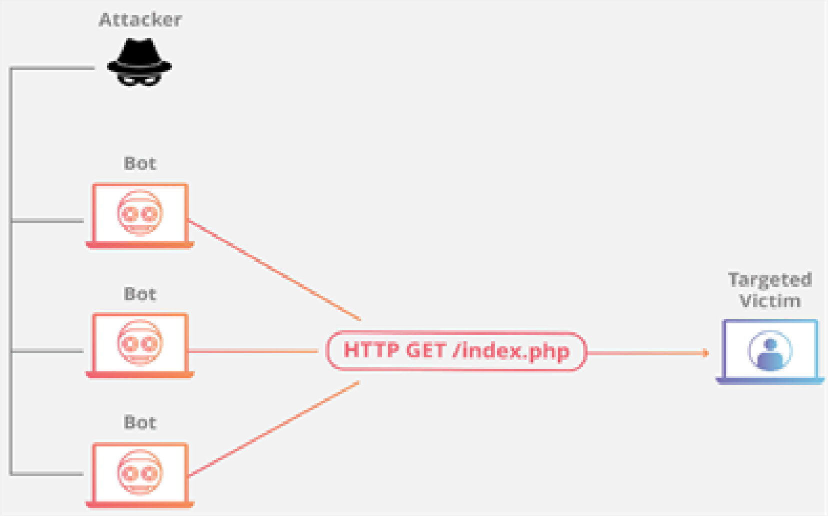

Fig 4:- Application Layer Attack Example HTTP Flood

This type of attack occurs because of reloading of the website by refreshing the website in the browser repeatedly. Refreshing the website multiple times resulting in firing the HTTP requests multiple times to the server, resulting in the denial-of-service.

This type of attack can be of two types - simple and complex. The simple HTTP flood attack includes attacking one URL with the same range of attacking IP addresses. The complex HTTP flood attack includes targeting the victim from more than one IP address. The victim can be random URLs.

- *Protocol Attacks*

Protocol attacks are also known as the state exhaustion attack. It causes a disruption in the normal service processes by consuming all the state capacity available of the web servers or intermediate resources like the load balancers and the firewalls. Protocol attacks take advantage of the third and the fourth layer of the protocol stack to render the target web servers inaccessible.

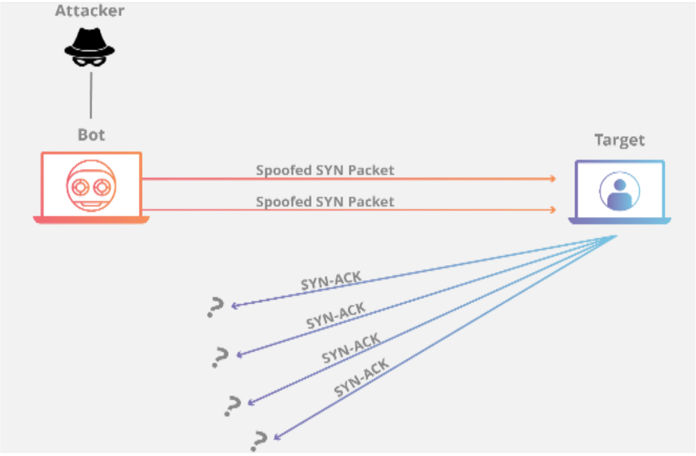

Fig 5:- Protocol attack example

- *SYN Flood*

A SYN flood is like the functioning of a worker at the store front. Considering this example, we can say that the function of the worker at the store front is to receive requests, get the packet and then waits for the confirmation order to bring the packet to the store front. The worker then gets many packet requests without the initial confirmation and keeps on getting the packets until it can hold no more, making the packet requests remain unanswered.

SYN flood attack exploits the TCP handshake protocol by sending many TCP connection request and SYN packets with spoofed IP addresses. The target machine responds normally to each connection requests and then waits for the final acknowledgement message from the recipient which never occurs. This ensures that the resources of the target machine get exhausted.

- *Volumetric Attacks*

This type of attack is used to create congestion between the target server and the larger internet by consuming all the available bandwidth. Large amounts of data are sent to the target web server by using a form of amplification or by creating enormous number of requests from the botnet.

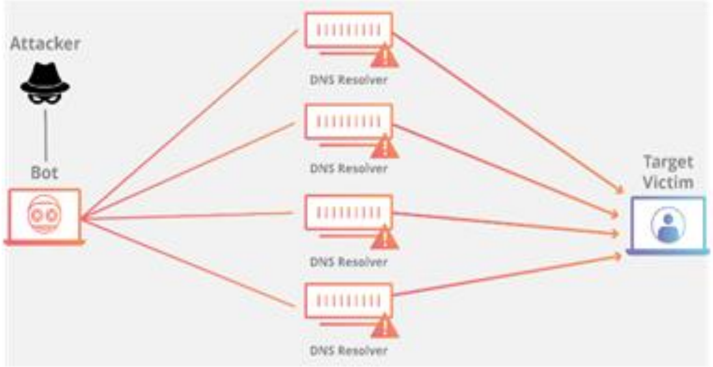

Fig 6:- Amplification example

VI. HOW TO HELP PREVENT DOS ATTACKS

The following are the steps which can be done to prevent the DDoS attack in the web server, network or the website -

Method 1: Recognizing the attacks

Technologies such as anti-DDoS services are often used to identify the DDoS attacks as they can differentiate between the legitimate requests in a network traffic and the DDoS attack.

Method 2: Contacting the Internet Service provider

Contacting the internet service provider in case of the attack. The internet service provider can help in re- routing the traffic. Alternative can be to have a backup ISP, which can be used to disperse the massive DDoS traffic from among the server networks.

Method 3: Investigating the black hole routing

Black hole routing is the process of directing excessive traffic to a null route. This null route is referred to as black hole. Internet service providers can perform the black hole routing. This is helpful in preventing the crashing of the targeted website or the server. The only drawback of this method is that both the legitimate and the illegal traffic is rerouted to the null route or the black hole.

Method 4: Configuring the firewalls and the routers

Firewalls and routers should be configured in such a way so that it removes the unnecessary traffic directed to the server or the network. Also, the firewall should be kept updated with the latest security patches.

Method 5: Installing the front-end hardware

Front end application hardware is integrated into the network to analyse and screen the traffic and the data packets before it reaches the server. The purpose of the hardware is to classify the data priority, regular, or dangerous while they enter a system. It can also help in blocking the threatening data.

REFERENCES

[1]. Research on DDoS Attacks Detection Based on RDF-SVM - Chenguang Wang ; Jing Zheng ; Xiaoyong Li

[2]. https://www.paloaltonetworks.com/cyberpedia/wh at-is-a-denial-of-service-attack-dos

[3]. Preventing Distributed Denial-of-Service Flooding Attacks With Dynamic Path Identifiers - Hongbin Luo ; Zhe Chen ; Jiawei Li ; Athanasios V. Vasilakos

[4]. https://us.norton.com/internetsecurity-emerging- threats-dos-attacks-explained.html

[5]. https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

[6]. https://www.cloudflare.com/learning/ddos/what- is-a-ddos-attack/

[7]. A survey of distributed denial-of-service attack, prevention, and mitigation techniques - Tasnuva Mahjabin, Yang Xiao, Guang Sun, Wangdong Jiang

[8]. Defence for Distributed Denial of Service Attacks in Cloud Computing – AndrewCarlin, MohammadHammoudeh, Omar Aldabbas

[9]. https://www.guru99.com/ultimate-guide-to-dos-attacks.html