ISSN No:-2456-2165

The Survey DDoS Attack Prevention and Defense Technique

Dr. L. Visalatchi
Associate Professor
Department of Information Technology
Dr.Umayal Ramanathan College for Women, Karaikudi.

PL. Yazhini
M.Phil Scholar
Department of Computer Science,
Dr.Umayal Ramanathan College for Women, Karaikudi

Abstract:- Without the security measures and controls, our data might be subjected to an attack. The DDoS attack is an attempt of attacking in a distributed fashion to make a server and its resources unavailable to its authorized users. The DDoS attack is a malicious attempt to disrupt access to the server by means of creating a large amount of traffic. In this paper, we propose types of DDoS attacks, analysis of different attacks so far, protection techniques and mitigation techniques, and possible limitations and challenges of existing research to reduce network overhead. Finally, some important research directions are given which require more attention shortly to ensure successful mitigation against distributed denial-of-service attacks.

Keyword:- *Types of DDoS Attack, Distributed Denial-of-Service Protection, Distributed Denial-of-Service Mitigation Technique.*

I. INTRODUCTION

Distributed denial-of-service attacks are a crisis to the internet. A DDoS attack requires a targeted machine which is termed as a victim and it requires to gain control of a network of a targeted machine (victim) to carry out the attack. If IoT devices are infected with malware, change each device is compromised which is referred to as bot. The attacker then has control over the group of bots and the DDoS

Attacks are usually accomplished by a group of compromised devices which are referred to as a botnet.

In distributed denial-of-service attacks(DDoS), attackers send a large number of breaches to the targeted system from different sources thus it not only prevents the authorized user from accessing the resources but also make it impossible to stop the flooding and it may also involve forging the IP address of the sender which further complicates in preventing the attack

Broadly speaking DDoS attacks are classified into three following methods:1. Sending the mountainous amount of thread to the server (Voluminous Attack) 2. Protocol Attacks 3. Application-level flooding. However, the protocol-based DDoS attacks are also classified based on the exploited vulnerability through which the attacker attacks the victim. In this mainly the network bandwidth of the victim is attacked through TCP, UDP, ICMP flooding. In the following sections, the common types of DDoS protocol attacks, Mitigation techniques, and defense methods are discussed and the observation made from the survey is presented with a conclusion.

II. TYPES OF DDoS ATTACK

There are the following types of DDoS attack.

- *Ping of Death:*

According to the TCP/IP protocol the maximum size of the packet can be 65535 bytes, the ping of death attack exploits this particular fact. In normal cases, a large IP packet is split into multiple fragments and the recipient host reassembles the fragments to make a complete packet. In the Ping of Death case, malicious manipulation is introduced by the attacker while reassembling the fragments and makes the packet size exceed more than 65,535 bytes. This results in the overflow of buffer memory allocated and therefore causes a denial of service for legitimate packets.

- *Smurf Attack:*

Smurf attacks use the whole network of computers to direct an overwhelming amount of traffic to a victim's machine and its network.

- Step 1: Attackers identifies a victim’s IP address.
- Step 2: Attackers will send an ICMP ECHO REQUEST containing a spoofed IP address which is actually the target server(Victim’s) address. This request is sent to all the network hosts on the network.
- Step 3: The host's ICMP ECHO RESPONSE on the network will be directed to the target victims' IP address.

With these voluminous responses forwarded the target victim is brought down.

- *HTTP Flood Attack:*

An HTTP flood attack is another mean of resource consuming attack. The main modes of HTTP flood attack are to manipulate the HTTP GET and HTTP POST requests while interacting with the target machine (victim). In order to achieve the connection, the attacker must have TCP connection with the valid IP address it can be achieved with the help of botnet. The attacker sends multiple requests from a botnet. In response to the request, it performs series of actions. Likewise using the memory of the targeted system and processing the power of the victim. A large

amount flood like this kind victim may not able to respond to the authorized user.

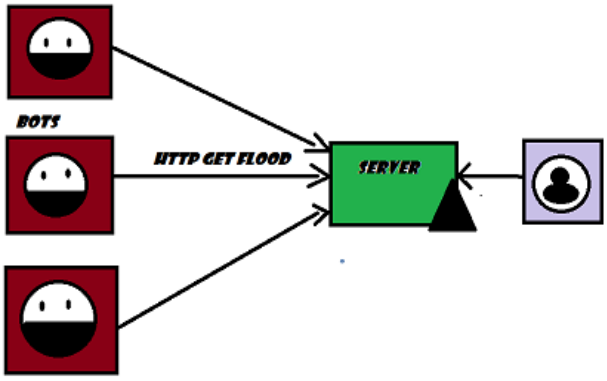

Fig 1:- HTTP Flood Attack

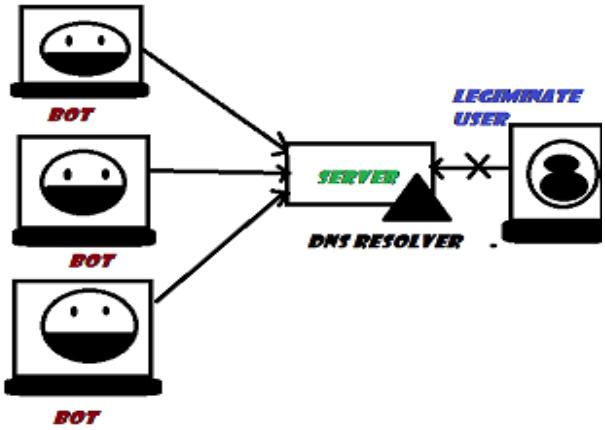

Fig 2:- DNS Flood Attack

➢ *UDP Flood Attack:*

UDP is the common protocol for live traffic communication. The attacker sends a large amount of a UDP packet onto a certain port on to the server. The server checks if there are any listening services at the port. If no services are listening on that UDP port, the servers respond to the client with an "ICMP host unreachable" packet. The attacker continuously sending a packet with a spoofed IP address to make victim resources unavailable or consume all its resources.

➢ *Synflood Attack:*

The SYN flood attack commonly called Threeway-handshake-method. Normally TCP connection has been made using the SYN-REQUEST packet to the host and response to the requestor using the SYN-ACK packet. In the SYN flood attack scenario, the requestor sends the SYN-REQUEST packet and response using ACK packet but it does not a response to the host's SYN-ACK packet, or sends SYN-REQUEST with the spoofed IP address or host system continuously waiting for ACK from requestor, it would not respond to the valid user resulting in denial-of-service.

➢ *DNS Flood Attack:*

Domain name system (DNS) is the "phonebook" of the internet through which internet devices can view a particular website to access internet content. The requestor sends an enormous amount of DNS requests to the victim the sole purpose is to overload it. In DNS flood attack host they connect to the internet can be affected due to the huge amount of traffic. The role of the botnet in the attack is to generate a large volume of traffic, for they need more than hundreds and thousands of infected systems (bots) with malware that might be under the control of the attacker.

III. MITIGATION TECHNIQUE

➢ *Detection:*

The first thing we do in the mitigation technique is to identify the network traffic it is defined by the "traffic patterns"; it is necessary for threat detection and alerting. The DDoS attack also clarifies that the incoming packet is human traffic or human-like bots and hijacking web browsers. It can be identified through the process of "comparing signature".

Comparing signature: In this comparing signature process, the IP address of each client is saved. It has a fingerprint for each legitimate user. Every incoming packet server must be done the process of comparing signature that means comparing the IP address of the legitimate user.

➢ *Rate Limiting:*

Rate limiting is the process of diminishing the network traffic. The number of requests to the server can be more during the attack. Through this kind of process, web scarabs noble the content. So that rate. For example, the server allows only 50 requests for one minute to access the content available on the server.

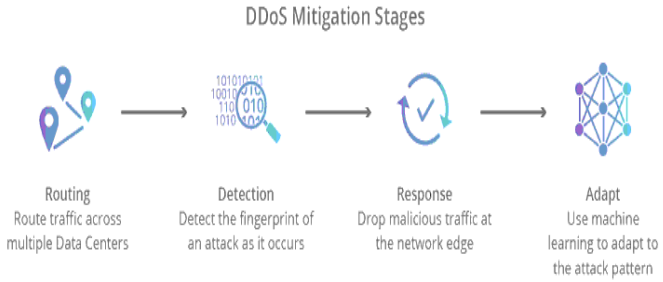

Fig 3:- DDoS Mitigation Stages.

IV. DEFENSE METHOD

➢ *New Cracking Algorithm:*

The new cracking algorithm in this we have three-technique to find the IP address spoofing.

- Packet filter
- Mac generator
- IP handler

The packet filter acts as intermediates for the packet transfer from the computer to the internet. If the packet matches with a set of the rules of packet filter that packet can be moved to the MAC generator. MAC generator distinguishes the packet which has a legitimate IP address. Once the first SYN packet from the client it redirects to the pseudo-IP address and port number pair, through the redirect URL message. Certain bits in the IP address and port number is the Message Authentication Code (MAC) for the client IP address. The attacker uses the genuine IP address, and then it passes to the deficit round-robin algorithm to collect the address of the client. If it is spoofed IP address it has been blacklisted and its signature is noted out. [8]

➢ *Instruction Detection System:*

It is the process of monitoring and analyzing the actions occur in computer and network to identify the network breach. There are two techniques in the IDS Anomaly detection technique and misuse detection technique. In the Anomaly detection technique software running information, operating system information and kernel information must match with the client. In the Detection technique, it matches every client with the attack signature which has been stored in the history.

The figure shows how the instruction detection system works, the client sends a packet to the server it can be checked out by IDS to confine that it is a valid user or not. If not access denied in the other case match the pattern with IDS components if it, not an attacker server will process the request. If it is forged it gathers the information about the attacker. [7]

➢ *Threeway Handshake Method:*

In the three-way handshake method, the attacker sends the SYN packet to the server sends the SYN-ACK package to the client for that packet client does not respond sever is in the half-open connection.

For then we use the "SYN Flood Protector" it is connected between server and internet. Firstly the three-way handshake is done between client and flood protector it is an authorized user then it transmits package to the client. If it is not a valid user flood protector does not transmit package to the server.

➢ *Ingress and Egress Filtering:*

Ingress filtering is used to verify the source IP address where it comes from. This filter allows only 12.168.1.0/24 source addresses, and the packet with 172.16.1.23 will not be allowed. This technique is mainly used in DDoS attack and this is the primary target of ingress filtering.

- *Ingress filtering* – filter out the packets before entering into the network.
- *Egress filtering*- filter out the packet before leaving your network.

Mainly it acts as a firewall in the network interface.

➢ *Path Identifying Mechanism (Pi):*

Pi (short for path identification), new kind of packet marking approach to find the IP address spoofing. Each packet is stamped with path route (en-route), job of the victim to find out packet traverse in the same path on the other hand it is IP address spoofing. The packet that travels on the same path has same identifier. The main role of the victim is to find all subsequent packets has been travel from the attacker by using filtration process.

On the other hand this method works well when half of the packet involved in the marking process. Prospect of different path will show the same path information. Thus it increases the possibility of false-positive and false-negative result. In this approach DDoS attack is modeled into two phases. In the first phase, the learning phase, the entire packet is to be unspecified so that we can analyze whether it is a legitimate user packet or packet is in the attack. That is to say, the victim is temporarily given the power to differentiate between authorized users' packets and attackers' packets. The victim is thus able to produce an attack markings list. In the second phase, the attack phase, the victim is no longer able to apply its packet identification function and is unavailable to use the Pi filter based on the information it has gathered in the learning phase. Pi method is more powerful packet marking approach. [1]

V. OBSERVATION

We can observe that many of the methods need to be implemented concurrently and collaboratively on several nodes, making them difficult to implement. In the Path Identification technique router's IP address that the Pi uses to mark the path is quite large to write into the packet's inadequate space. The disadvantage of writing routers' IP addresses into the inadequate space may result in the same path identification for different paths. With these annotations and concerns in mind, implementing an effective defines method becomes a serious investment that requires serious concern to reach a balance between benefits and costs: the location, simplicity, performance, and cost of a defense system are associated and an efficient system is one which optimizes these factors.

VI. CONCLUSION

The survey of the all relevance prevention and defense techniques against DDoS with IP forge we can conclude that methods may be different in the region, the amount of legitimate traffic they control, their ease of implementation, and the type of attack they are successful against, every method has certain features that make it more appropriate to implement in one condition than another.

REFERENCES

[1]. T Mahjabin, Y Xiao, G Sun… - International Journal of …, 2017 - journals.sagepub.com. *A survey of a distributed denial-of-service attack, prevention, and mitigation techniques.* In: International Journal of Distributed Sensor Networks 2017, Vol. 13(12) The Author(s) 2017 DOI:10.1177/1550147717741463 journals.sagepub.com/home/dsn.

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

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

[4]. Simona RAMANAUSKAITĖ "Modeling and research of Distributed Denial of service attack ".

[5]. 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.

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

[7]. 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.

[8]. V.Priyadharshini, Dr.K. Kuppusamy" *Prevention of DDOS Attacks using New Cracking Algorithm*" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.2263-2267.

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

[10]. Wikipedia. Internet activism during the 2009 Iranian election protests—Wikipedia, the free encyclopedia, 2017, https://en.wikipedia.org/w/index.php?title=Internet_activism_during_the_2009_Iranian_election_protests&oldid=769078109(accessed 10 March 2017).

[11]. Srivastava A, Gupta B, Tyagi A, et al. A recent survey on DDoS attacks and defense mechanisms. In: NagamalaiD, Renault E and Dhanushkodi (eds) Advances in parallel distributed computing. Berlin; Heidelberg: Springer,2011, pp.570–580.

[12]. Specht SM and Lee RB. Distributed denial of service: taxonomies of attacks, tools, and countermeasures. In: Proceedings of the ISCA 17th international conference on parallel and distributed computing systems (PDCS 2004), an international workshop on security in parallel and distributed systems, San Francisco, CA, 15–17 September 2004,pp.543–550. IEEE.

[13]. Netcraft. Web server survey, 2017, https://news.netcraft.com/archives/category/web-server-survey/ (accessed 1 April 2017).

[14]. Gao J and Xiao Y. ProtoGENI DoS/DDoS security tests and experiments. In: Proceedings of the 1st GENI research and educational experiment workshop (GREE12), in conjunction with GENI GEC 13, Los Angeles, CA, 13–15 March 2012.

[15]. SecurityIQ. Cheating VoIP security by flooding theSIP,2016,http://resources.infosecinstitute.com/cheating-voipsecurity-by-flooding-the-sip/#gref (accessed 13 April 2017).

[16]. Patrick Park NW. Call flooding attack, 2009, http://www.networkworld.com/article/2234402/cisco-subnet/callflooding-attack.html (accessed 13 April 2017).

[17]. Graham-Cumming J. Understanding and mitigating NTP based DDoS attacks, vol. 9. San Francisco, CA: Cloudflare, Inc., 2014.