A Survey and New Perspectives on Classifying the DDOS Attack with Their Characteristics

[1]M.Jeyaraman,
Pg And Research Department Of Mathematics,
Raja Doraisingam Govt, Arts College,
Sivagangai-630561, Tamil Nadu, India.
Jeya.Math@Gmail.Com

[2]R.Saravanaprabu
Assistant Professor, Dept.Of Mathematics
Nms.Svn College
Madurai, Tamil Nadu, India.
R.Saravanaprabu@Gmail.Com

Abstract:- In network Distributed Denial of Service (DDoS) attacks has been a major threat to the Internet society. The DoS attack produces a large number of client bases due to the enslavement of major users on Web society. In such a DoS attack, the malicious invader targets a system to corrupt its services to the proposed users. These types of attacks are mainly motivated by the existence of different groups of hackers and crackers present on the network. The current research has progressed in this field; researchers have come across many ways through which attacks have been successfully launched. In early days of its origin, the Internet was not planned to face different vulnerable problems, in this aspect networks are need to protect. In this research paper covers the initiation of the DDoS attacks together with their types, and also deliberate certain model scenarios based on flooding based DDoS attacks to compute its impact on valid users and also we classified the different types of DDoS attacks with their environment and tabulated the results.

Keywords: *DoS, SYN flood, flooding, DDoS Defense.*

*****

I.INTRODUCTION

A Denial of Service (DoS) attack can be discriminate as an attack with the reason of avoid valid users from using a victim computing system or network resource [1]. The Distributed Denial of Service (DDoS) attack is a main synchronized attack on the accessibility of services of a victim system or network system, initiated indirectly through many conciliation computers on the Internet. The services in attack are those of the "major victim", while the conciliation systems used to begin the attack are often called the "tangential victims". The utilization of tangential victims in performing a DDoS attack gives the attacker with the skill to wage a much larger and more riotous attack, while making it more intricate to track down the novel attacker **[2].**

II.TYPES OF DDoS ATTACKS [3]

SYN FLOOD

SYN flood is a kind of DoS attack in which an attacker intentionally sends a sequence of SYN requests to a target system in an effort to consume adequate server resources to construct the system impassive to legitimate traffic.

ACK or ACK-PUSH Flood

When the link between the host and the ACK or the PUSH ACK client is recognized, data packets are used to transmit data both ways till the session ends. The victim server molest by an ACK flood receive fake ACK packets that do not belong to any of the sessions time on the server's list of communication. The server may under attack then squander all its system resources trying to identify where the fabricated packets belong. This type of attack may cause efficiency loss and partial server unavailability.

FRAGMENTED ACK FLOOD

In a fragmented ACK flood attack, a comparatively small number of maximum size packets used to fill bandwidth. In a fragmented ACK packets simply pass through routers, filters and intrusion prevention systems, as these devices do not recompile the fragmented packets on the network levels. Typically, such data packets contain random data. The attacker aims to fill the entire network bandwidth of the victim's external network, this type of flood attack reduce the performance of all the servers in the targeted networks.

RST/FIN FLOOD

In TCP-SYN session, there should be exchange of RST or FIN packets between both the client and the host. At the time of an RST / FIN Flood attack, the victim server is continuously send with fake RST or FIN packets that have no connection are to any of the sessions stored in the server's database.

FAKE SESSION ATTACK

The attacker creates fake SYN-packets that are tag along by a lot of ACK, and at last FIN/RST packets. All these packets look like real TCP session traffic that is being sent from one host to another.

UDP FLOOD

UDP flood attack is a DoS attack using the User Datagram Protocol (UDP), a session less/connectionless computer networking protocols. Using UDP for DoS attacks is uncomplicated as with the Transmission Control Protocol (TCP).

UDP FRAGMENTATION

An UDP application may wish to shun IP fragmentation, because when the packet size of the resulting datagram goes above the link's Maximum Transmission Unit, the IP datagram is divide across multiple Internet Protocol packets, which can direct to recital issues because if any fragment is gone, the entire datagram is lost.

ICMP FLOODING

An ICMP Flooding attack the data sending of a strangely huge volume of ICMP packets of any type can overcome a target server that endeavor to process every inward ICMP request, and this can result in a DoS condition for the target servers.

PING FLOOD

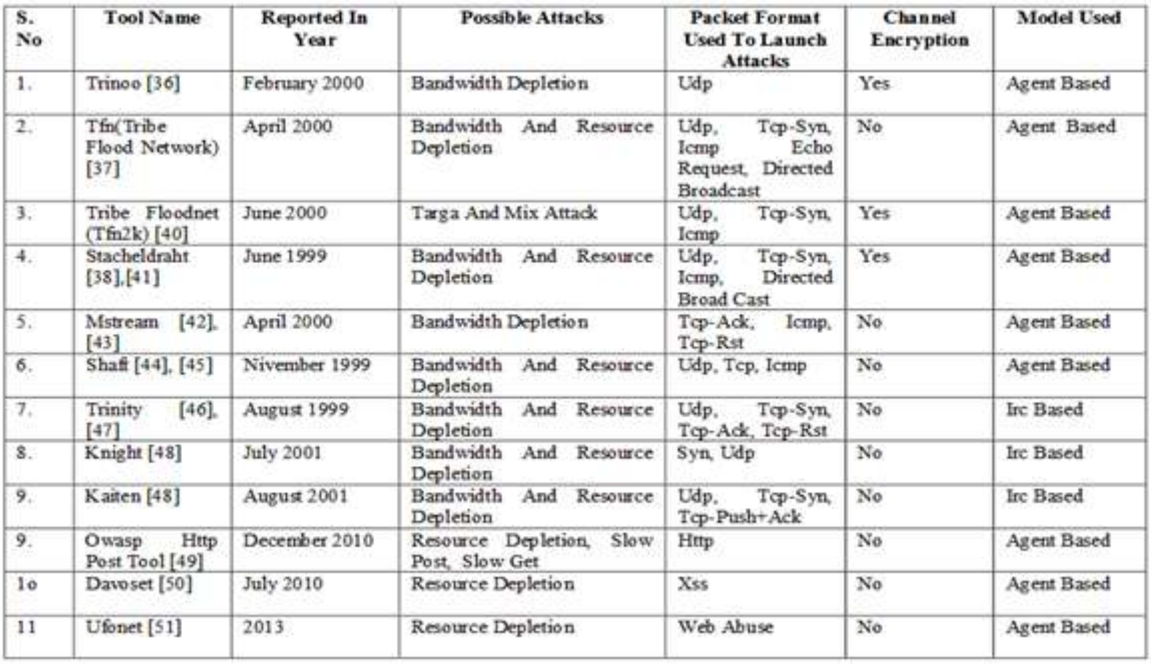
A ping flood is a simple DoS attack where the attacker overcomes the victim with ICMP Echo request packets. This is most efficient by using the flood option of ping which throws ICMP packets as fast as feasible without waiting for replies

DNS FLOOD DNS AMPLIFIED

The DNS flood attacks must be clearly distinguish from DNS amplifications attack. DNS amplifications is an asymmetrical Distributed Denial of Service attack in which the attacker can sends out a small lookup query with the spoofed target IP address, making the spoofed target the receiver receives a large amount of DNS responses. With these types of attacks, the attacker's aim is to saturate the network resource by incessantly grueling bandwidth capability.

III COMPARISION OF DDOS TOOLS[4]

TABLE 1:Comparision of DDoS tools



S. No	Tool Name	Reported In Year	Possible Attacks	Packet Format Used To Launch Attacks	Channel Encryption	Model Used
1.	Trinoo [36]	February 2000	Bandwidth Depletion	Udp	Yes	Agent Based
2.	Tfn(Tribe Flood Network) [37]	April 2000	Bandwidth And Resource Depletion	Udp, Tcp-Syn, Icmp Echo Request, Directed Broadcast	No	Agent Based
3.	Tribe Floodnet (Tfn2k) [40]	June 2000	Targa And Mix Attack	Udp, Tcp-Syn, Icmp	Yes	Agent Based
4.	Stacheldraht [38],[41]	June 1999	Bandwidth And Resource Depletion	Udp, Tcp-Syn, Icmp, Directed Broad Cast	Yes	Agent Based
5.	Mstream [42], [43]	April 2000	Bandwidth Depletion	Tcp-Ack, Icmp, Tcp-Rst	No	Agent Based
6.	Shaft [44], [45]	Nivember 1999	Bandwidth And Resource Depletion	Udp, Tcp, Icmp	No	Agent Based
7.	Trinity [46], [47]	August 1999	Bandwidth And Resource Depletion	Udp, Tcp-Syn, Tcp-Ack, Tcp-Rst	No	Irc Based
8.	Knight [48]	July 2001	Bandwidth And Resource Depletion	Syn, Udp	No	Irc Based
9.	Kaiten [48]	August 2001	Bandwidth And Resource Depletion	Udp, Tcp-Syn, Tcp-Push+Ack	No	Irc Based
9.	Owasp Http Post Tool [49]	December 2010	Resource Depletion, Slow Post, Slow Get	Http	No	Agent Based
1o	Davoset [50]	July 2010	Resource Depletion	Xss	No	Agent Based
11	Ufonet [51]	2013	Resource Depletion	Web Abuse	No	Agent Based

TABLE: 2 COMPARISION OF DDOS DEFENSE MECHANISMS

S.No.	DEFENSE MECHANISM	ADVANTAGES	SHORTCOMINGS
1	Ingress/Egress filtering at sources edge routerD-WARD	Detect and filter packets with spoofed IP addresses at the sources edge routers based on the valid IP address range internal to the network	Spoofed packets will not be detected if their addresses are still in the Valid internal IP address range
2		Stop attack traffic originating From a network at the border of the source network	It consumes more memory space and CPU cycles than some of the network-based defense mechanisms
3	MULTOPS	Detects and Filters ddos flooding attacks based on significant difference between the rates of traffic going to and coming from a host or subnet	It uses a dynamic tree structure for monitoring packet rates for each IP address which makes it a vulnerable target of a memory exhaustion attack
4	Packet marking and filtering mechanisms	Mark legitimate packet sat each router along their path to the destination so that victims‟ edge routers can filter the attack traffic	Dependent in part on the strength of the attackers, and when it increases, filters become ineffective and they cannot properly be installed
5	Reducing SYN-RECEIVED Timer	Put a tighter limit on the amount of time between when a TCB enters the SYNRECEIVED state and when it may be reaped for not advancing	In cases of aggressive attacks that impose some amount of congestion loss in either the SYN-ACK or handshake completing ACK packets, legitimate connection tcbs may be reaped as hosts are in the process of retransmitting these segments

IV RISKS ASSOCIATED WITH DENIAL OF SERVICE ATTACKS [5]

Denial of Service attacks is centered on the concept that by overloading a target's resources, the system will ultimately crash. In the case of a DoS attack against a web application, the software is overloaded by the attack and the application fails to serve web pages properly. To crash a web server running an application, a DoS threat attacks the following services:

- Network bandwidth
- Server memory
- Application exception handling mechanism
- CPU usage
- Hard disk space
- Database space
- Database connection pool

In the past, Denial of Service attacks were thought to be a tool used by hacktivists as a form of protest. However recent attacks have shown that Denial of Service attacks can also be way for cyber criminals to profit.

By not proactively working to prevent Dos attacks, you leave your site vulnerable to:

- Extortion: Attackers threaten to continue disrupting service until payment is received.
- Sabotage: Competing businesses attack web sites to build a stronger market share.
- Brand damage: Sites that are attacked find that their reputation is hurt by lack of uptime or the perception that the site is not secure.
- Financial losses: Sites that are attacked are prevented from doing business online. The result is often a loss in sales revenue or advertising revenue.
- Other attacks: Information gathered from a successful Denial of Service attack can be used later to further attack a web site. Additionally, other vulnerabilities may be used to launch a DoS attack providing the attacker with access to more than they had originally intended.

V PREVENTIVE MECHANISM [6]

Individual Users. One of the best methods to prevent DDoS attacks is for the secondary victim systems to prevent themselves from participating in the attack. This requires a heightened awareness of security issues and prevention techniques from all Internet users. If attackers are unable to break into and make use of secondary victim systems, then the attackers will have no “DDoS attack network” from which to launch their DDoS attacks.

In order for secondary victims to not become infected with the DDoS agent software, users of these systems must continually monitor their own security. They must check to make sure that no agent programs have been installed on their systems and that they are not sending DDoS agent traffic into the network [7]. Many corporate websites have suffered from illegal denial-of-service (DoS) attacks more than once. The companies that learn how to turn these experiences to their advantage go a long way to ensuring it doesn't happen again. Sometimes there's nothing like adversity to give you a new look at your surroundings. And the events of a network attack can uncover some very important mistakes and provide you

With more than a few lessons. Turning these lessons into best practices is where the rewards of such adversity are realized. You can arrive at these best practices by asking yourself: "How are we vulnerable?" The following best practices are a sample of some of the common conclusions companies have come to following a DoS attack.

Practice 1	Keep an audit trail that describes what was changed and why.
Practice 2	Create interdepartmental Standard Operating Procedures (SOPs) and Emergency Operating Procedures (EOPs).
Practice 3	Understand that success can result in complacency.
Practice 4	Network monitoring isn't enough; your administrators must know your configuration in detail.
Practice 5	Test yourself both locally and over the Internet.
Practice 6	Your processes can harm you just like as hackers.
Practice 7	Keep people aware of old configurations and their purpose.
Practice 8	When something is different, ask why.
Practice 9	Know the trade-offs between simplicity, cost, and survivability.
Practice 10	Protect yourself against hackers.

VI CONCLUSION

DDoS attacks are fairly high advanced and potent methods to attack a network system to create it either ineffectual to the valid users or reduce its performance. They are ever more mounted by professional hacks in barter for benefits. This survey inspects the probable solutions to this quandary, gives classification to order those solutions and examine the possibility of those approaches. Based on the analysis of existing solutions, we proposed advantageous solutions to defend DDoS.

VII REFERENCES

[1] David Karig and Ruby Lee, “Remote Denial of Service Attacks and Countermeasures,” Princeton University Department of Electrical Engineering Technical Report CE-L2001-002, October 2001.

[2] Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures Stephen Specht and Ruby Lee Princeton Architecture Laboratory for Multimedia and Security (PALMS) Department of Electrical Engineering Princeton University

[3] https://www.corero.com/resources/Glossary.html

[4] Rajkumar , Manisha Jitendra Nene A Survey on Latest DoS Attacks: Classification and Defense Mechanisms, International Journal of Innovative Research in

Computer and Communication Engineering Vol. 1, Issue 8, October 2013

[5] http://www.applicure.com/solutions/prevent-denial-of-service-attacks

[6] Taxonomies of Distributed Denial of Service Networks, Attacks, Tools, and Countermeasures

[7] https://msdn.microsoft.com/en-us/library/cc750213.aspx

[8] P.Vadivelmurugan ,K.Alagarsamy Cataloguing and Avoiding the Buffer Overflow Attacks in Network Operating Systems , International Journal of Computer & Organization Trends –Volume 3 Issue8 – Sep 2013

[9] P.Vadivelmurugan ,K.Alagarsamy Securing Server System from Buffer Overflow vulnerability using Vel-Alagar Algorithm, International Journal of Mathematics Trends and Technology- Volume4 Issue 9 - October 2013