DDoS Tools: Classification, Analysis and Comparison

Bharti Nagpal
Asstt. Professor (CSE Deptt.),
AIACT&R, Delhi, INDIA
Email Id: bharti_553@yahoo.com

Pratima Sharma
AIACT&R,
Delhi, INDIA
Email Id: pratima.sharma1491@gmail.com

Naresh Chauhan
Professor (CSE Deptt.), YMCAUST,
Faridabad, INDIA
Email Id: nareshchauhan19@yahoo.com

Angel Panesar
Student, AIACT&R
Delhi, INDIA
Email Id: angelpanesar@gmail.com

Abstract – Distributed Denial of Service (DDoS) attacks are the major concern for the security experts. DDoS attack presents a serious risk to the internet. In this type of attack a huge number of accommodated targets send a request at the victim's site simultaneously, to exhaust the resources (whether computing or communication resources) within very less time. In the last few years, it is recognised that DDoS attack tools and techniques are emerging as effective, refined, and complex to indicate the actual attackers. Due to the seriousness of the problem many detection and prevention methods have been recommended to deal with these types of attacks. This paper aims to provide a better understanding of the existing tools, methods and attack mechanism. In this paper, we commenced a detailed study of various DDoS tools. This paper can be useful for researchers and readers to provide the better understanding of DDoS tools in present times.

Keywords – DDoS, DDoS attack methods; DDoS attack tools, DDoS defences.

NOMENCLATURE

DDoS: Distributed Denial of Service attack.
TFN: Tribal Flood Network tool used for launching a DDoS attack to a target.
LOIC: Low Orbit Ion Cannon is an automatic DDoS tool.
ICMP: Internet Control Message Protocol packet.

I. INTRODUCTION

Internet has turned into the demand of current association. The internet architecture focussed on performance and not the security. Novice users leave their systems vulnerable to compromise. For example: using easy and general passwords, leaving design features in default mode, switching off firewalls etc. All these weaknesses making easily access root information by the attacker. Denials of Service attacks are very frequent in the cyberspace world. Increasing use of distributed

Denial of Service attack has made the computer and network services at greater risk than ever before. Therefore, to mitigate the effects of cyber-attacks including DDoS some organization and people are making plans and investments in order to secure their utilities or services.

The DDoS is an attacking approach in which attacker send a huge number of requests to victim system by regulating the accommodated host for the motive of damaging and disrupting the resources of the target hosts. Distributed Denials of Service attack do not depend on specific rules or vulnerabilities. Rather, they easily damage the huge utilities by accommodating the multiple hosts to send the packets to the victim's machine at the same time. Many schemes give various detection methods. However, there is no perfect method that detects as well as prevents DDoS. Therefore, the stopping of DDoS attack is a challenging issue and to make differentiation between the useless traffic and the genuine traffic become the main responsibility.

DDoS is a severe problem to the availability of cyberspace utilities. They have damaged the services of individual host including main commercial since and even the infrastructure services. DDoS attacks may cost a victim site loss of millions of dollars by making them non available for hours. The DDoS tools do not require technical knowledge to execute them. Hence DDoS are becoming easier to launch and difficult to detect.

In this paper, we studied the various DDoS attacking tools so that we know the trend of attacking method used by the attackers to launch an attack. This paper also helpful to identify the various defence techniques against these attacks.

978-9-3805-4416-8/15/$31.00

II. DISTRIBUTED DENIAL OF SERVICE

It is an attack in which multiple compromised computers are used to flood the victim servers, with a large number of packets and block them so that resources are inaccessible by the authorized users. Most of the time, the owners of the compromised hosts does not realize that they are being used by attackers. In some examples, attackers only flood the web servers in order to damage the utility, on the contrary of taking it down fully. Therefore, now a day DDoS attacks are the major concern for securing the systems present in the cyberspace world As shown in Figure 1 the DDoS attack consists of four main segments – an attacker, controller, zombies and a victim and is taken place in multiple steps. The attacker compromises the multiple hosts for launching a DDoS attack to the target machine. The attacker uses the single source machine for attacking the target and also handles all the compromised machines by using remote authentication in order to command them to send the multiple requests at the same time so that it depletes the bandwidth and resources of the target machine. In this process handler uses multiple agents or daemons for sending the multiple request at the particular instant of time. In the way attackers overwhelm the victim hosts or routers, making them incompetent of providing utilities.

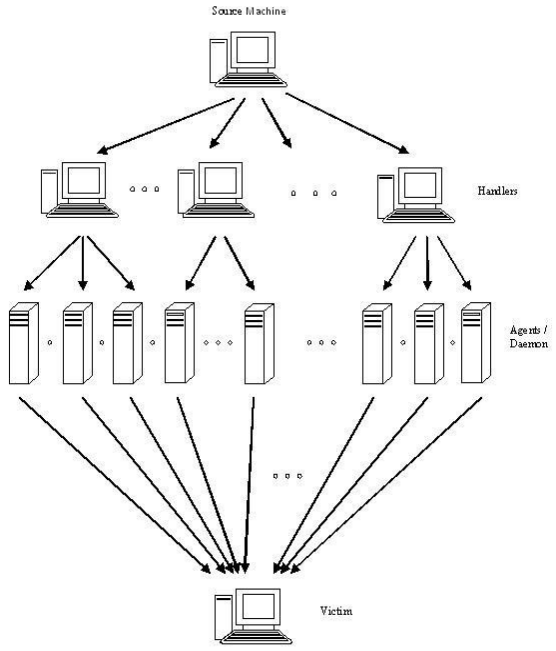

Fig.1. Architecture of DDoS [2]

III. TYPES OF DDoS ATTACK

DDoS Attacks classified into two types: direct and reflector attacks. In direct attacks, compromised hosts execute an attack on the target directly whereas in reflector attacks, compromised hosts send packets for request with spoofed IP address that is; IP of the target machine is present in source address field of IP packets.

A. Direct Attacks

In a direct attack, the victim is overwhelmed by large number of packets sent directly by the attacker (as in Fig. 2.). Types of attack packets may be TCP, ICMP, UDP, or a mixture of them. Various methods used to implement the attack include SYN Flooding, RST Flooding and ICMP Flooding. The methodologies are briefly explained in Table I.

Another aspect is IP traceback. IP traceback is the process in which identification of the original sender of the packet across the Internet is done, without depend upon the source detail in the packet. IP traceback is possible in direct attacks but not when the DDoS attack is being performed. This can be done after the attack has been performed.

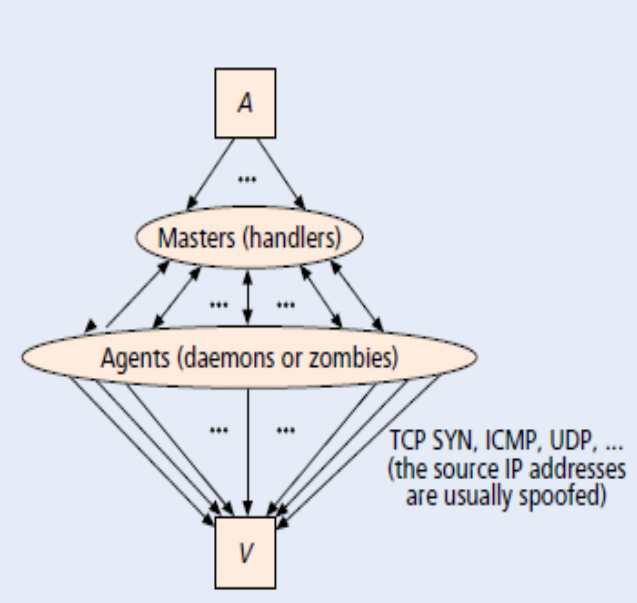

Fig.2. Architecture of Direct Attacks [12]

B. Reflector Attacks

A reflector attack is performed by using mediator like routers, called *reflectors*, are purposely implemented as attack launchers (as in Fig. 3.). Same methods used for direct attacks can be used to implement reflector attacks also but these attacks use a different methodology. These methodologies are briefly explained in Table I.

Traceback mechanism is unable in reflector attacks because it uses reflectors to send the packets at the target machine by using spoofing. Even if the attacker may be successfully identified, it is a complex process to stop them from sending

attack packets. Further, if that tracing is finished using a process that depends on continuously sniffing high volume of spoofed traffic e.g., ITRACE, then the attacker may suppress the tracing by growing each captive's traffic through multiple routers which considerably increases the time required by tracing process to collect adequate traffic to analyse.

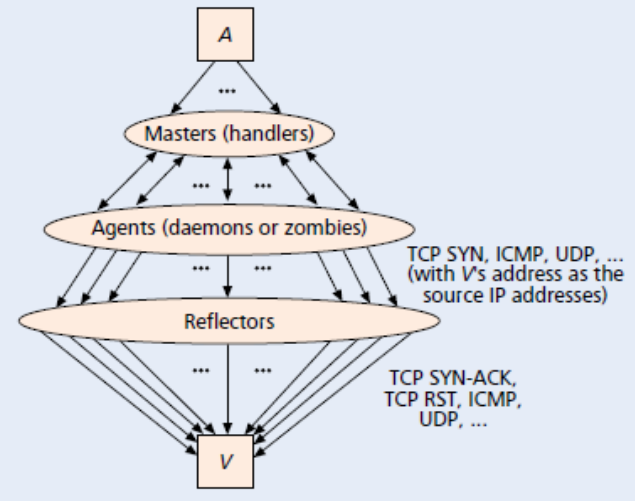

Fig.3. Architecture of Reflector Attacks [12]

C. Methodologies

TABLE I. DIRECT VS REFLECTOR ATTACK

TYPE / METHOD	DIRECT ATTACK[12, 13]	REFLECTOR ATTACK[12, 13]
Method 1: SYN Flooding	In this kind of flooding, a large number of TCP SYN packets are sent to an active port of the victim. If the port is constantly active for requests for connection, the victim will reply by sending SYN-ACK packets as an acknowledgement. But since spoofed addresses are used as a source address in these attack packets, these reply packets are sent somewhere else in the cyberspace. So, the victim resends the SYN-ACK packets a huge number of times. These will instantly consume all the resources and the victim will not be able to accept new requests.	TCP SYN packets are sent by the attacker to the TCP Servers by using the victim's IP address as the source address in the TCP packet so that reflector sends the TCP SYN-ACK packets as a response to the target machine.
Method 2 : RST Flooding	RST Flooding includes congesting a victim's entering link. In order to make the victim to reply with RST packets.	TCP packets are sent to non-listening TCP ports and the reflector sends TCP RST packets to the victim.
Method 3: ICMP Flooding	ICMP packets and UDP packets are mostly used. In these, the victim response back by generating the corresponding reply for ICMP and UDP packets.	ICMP queries (usually echo queries) are sent by the attacker to the reflector and reflector sends ICMP replies (usually echo replies) to the victim.

IV. DDOS ATTACK TOOLS

In this paper, most popular tools are studied, and compared. DDoS attack happens not only for wired architecture but also for wireless environments. Various different tools or methods are used to scan infected and vulnerable machines, but only a few DDoS tools are able to reach at the required phase. Most common DDoS tools like Tribal Flood network (TFN), Trin00, Low orbit ion cannon (LOIC), Trinity and Mstream. These tools differ in terms of architecture used, types of channel encryption technique and deployment method. In Table 2, we compared the various tools on the basis of type of flooding; architecture used and channel encryption in order to increase the better understanding of these tools that helpful in future to protect the vulnerable systems.

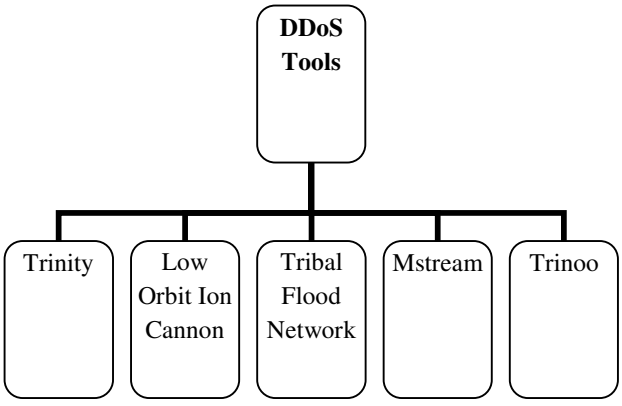

Fig. 4

TABLE II. COMPARISON ANALYSIS OF DDOS TOOLS

TOOLS / TERMS	TFN[3]	TRINOO[6]	MSTREAM[4]	LOIC[8]	TRINITY[5]
Definition	TFN is a DDoS tool using the UDP flood, Smurf attack, TCP SYN flood for launching the attack at the victim's site. TFN used cmd interface to connect the intruder and the automatic program in order to launch a DDoS attack but it does not use encryption between agents and handlers or attackers and handlers	Trinoo is a bandwidth depletion tool that can be used to launch an attack by using UDP flooding to attack against one or more IP addresses. The tool uses fixed sized UDP packets to target active ports on the target computer. A previous version of trin00 supports IP source address spoofing.	The Mstream tool uses spoofing method for attacking the target host. For example using imitated TCP Acknowledge packets to attack the victim's site. Mstream tool uses TCP ACK floods that, as a reaction, can swamp the information used by routing methods in switches.	Low Orbit Ion Cannon (LOIC) is an attacking tool that is easily and freely available to attack on victim's site. LOIC launch a DDoS attack by using the various flooding method e.g. TCP, UDP and ICMP in order to damage the resources such as CPU time, storage and bandwidth of the compromising host.	Trinity is a tool that utilises the UDP, TCP SYN, TCP Acknowledge and TCP NULL packet flooding to attack the site. It also introduces various new flooding methods like TCP fragment, TCP RESET packet and transmission control protocol random flag packet flooding methods to attack the victim's site.
Architecture used	Agent based	Agent based	Agent based	Agent based	IRC based
Type of Flooding used for attacking	UDP, TCP SYN, ICMP echo request and direct broadcast address	UDP	TCP SYN , ICMP and RST	TCP SYN, UDP, ICMP	UDP, TCP SYN, ICMP
Types of DDoS method used	Direct method	Direct method	Direct method	Direct method	Direct method
Possible damage caused	Bandwidth and Resource depletion	Bandwidth depletion, Remote Buffer overrun exploitation	Bandwidth Depletion	Resource and Bandwidth depletion	Resource and Bandwidth depletion
Channel encryption	Communication channel between the attacker and handlers is encrypted using CAST-256 algorithm.	Communication channel can use encryption and password protection as well.	Communication is not encrypted	Encryption used during communication	Communication is not encrypted

V. CONCLUSION AND FUTURE SCOPE

With time, more and more population is starting to use internet. Internet has reached such places where people could not even think that such kind of network exists which provide any possibly imaginable information. With the increased use of internet, a large number of attackers are keeping an eye to launch attacks to get access to critical information and even crash the complete servers. There are various vulnerable systems on the Internet that can be used for launching DDoS attacks. And, DDoS attacks are very difficult to defend against in spite of using defense mechanisms and will be an effective form of attack. In this paper, we present DDoS in detail, types of DDoS attacks have been explained in tabular form. We also provide a review on some common tools used to launch DDoS attacks. These tools do not require any technical knowledge as these are automated can be used by a naïve user too. Future scope can include various defense mechanisms for the DDoS attacks launched by various tools explained in this paper.

REFERENCES

[1] Arun Raj Kumar, P. and S. Selvakumar, "Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms", *International Advance Computing Conference (IACC 2009)*, pp 1275-1280, March 2009.

[2] Poongothai and Sathyakala,"Simulation and Analysis of DDoS Attacks", *International Conference on Emerging Trends in Science, Engineering and Technology,* pp 78-85, 2012.

[3] D. Dittrich, "The Tribe Flood Network Distributed Denial of Service attack tool", University of Washington, October 21, 1999.

[4] D. Dittrich, G. Weaver, S. Dietrich, N. Long, "The Mstream Distributed Denial of Service attack tool", May 2000.

.

[5] B. Hancock,"Trinity v3, a DDoS tool", Computers Security 2000.

[6] P.J. Criscuolo, "Distributed Denial of Service TrinOO, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht CIAC-2319", Department of Energy Computer Incident Advisory (CIAC), Rev., Lawrence Livermore National Laboratory, February 14, 2000.

[7] Saman Taghavi Zargar, James Joshi, and David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", *IEEE Communications Surveys & Tutorials*, Vol. 15, No. 4, pp. 2046-2068, 2013.

[8] Praetox Technologies *Low Orbit Ion Cannon*, 2010, [online] https://github.com/NewEraCracker/LOIC/

[9] Joao B. D. Cabrera, Lundy Lewis, Xinzhou Qin, Wenke Lee and Raman K. Mehra "Proactive Intrusion Detection and Distributed Denial of Service Attacks—A Case Study in Security Management,", *Journal of Network and Systems Management*, Volume 10, Number 2: pp. 225-254, July 2002.

[10] Alex Doyal, Justin Zhan and Huiming Anna Yu, "Towards Defeating DDoS Attacks", *International Conference on Cyber Security,* pp. 209-211, 2012 IEEE.

[11] S. karthik, R. M.Bhavadharini and V.P Arunachanlam, "Analysing Interaction between Denial of Service attack and threats", *International Conference on Computing, Communication and Networking (ICCCN)*, 2008.

[12] Rocky K. C. Chang, "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial", *IEEE Communications Magazine*, pp. 42-51, October 2002.

[13] AT&T Center for Internet Research at ICSI *An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks*, [online]http://www.icir.org/vern/papers/reflectors.CCR.01.pdf.

[14] Jiang Feng, "The Research of DDoS Attack Detecting Algorithm Based on the Feature of the Traffic", *5th International Conference on Wireless Communications Networking and Mobile Computing*, 09/2009