IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203048 |

DDoS Tools: Classification, Analysis and Comparison

[1]B. Darahaas Kiran, [2] Dr. Ganesh D

[1]PG Student, School of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India

[2] Professor, Department of School of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India.

ABSTRACT: The primary worry of security specialists is assaults that cause denial of service. Attacks known as distributed denial of service (DDoS) pose a major threat to the internet. This type of attack aims to quickly exhaust all available resources, including computer and communication resources, by having several permitted targets simultaneously send requests to the victim's location. The sophistication, effectiveness, and usefulness of DDoS attack tools and techniques in identifying the actual offenders has been recognized in recent years. Numerous detection and preventive techniques have been suggested to cope with these kinds of attacks due to the severity of the issue. Enhancing understanding of the instruments, methods, and assault mechanisms now in use is the aim of this effort. In the beginning of this article, we started

KEYWORDS*:* DDoS, DDoS attack techniques; DDoS assault instruments; DDoS protections.

I. INTRODUCTION

The internet is becoming a need for modern associations. The internet was designed with performance in mind rather than security. Users without experience leave their systems vulnerable to attack. Use straightforward, globally applicable passwords, leave design elements in their default settings, disable firewalls, etc. as examples. With all these vulnerabilities, root information is easily obtained by an attacker. In the online community, denial-of-service attacks are frequent.

Due to the possibility of denial-of-service attacks, computer and network services are now more vulnerable.. As a result, some organizations and individuals are planning ahead and investing in order to defend their utilities or services in order to lessen the effects of cyberattacks, particularly DDoS attacks.

In order to harm and disrupt the resources of the target hosts, a DDoS attacker sends a massive volume of requests to the victim system by controlling the accommodating host. Attacks known as distributed denial of service are not dependent on any particular guidelines or weaknesses. Instead, they just destroy the massive utilities by allowing several hosts to simultaneously transmit packets to the victim's computer. Several techniques offer different ways to detect things. Nevertheless, there's no foolproof way to identify and stop DDoS attacks. As such, preventing DDoS attacks is a difficult problem, and the primary duty now is to distinguish between legitimate and worthless communications.

DDoS poses a serious threat to the accessibility of online services. They have harmed both infrastructure services and the services provided by specific hosts, including major commercial networks. A vulnerable site may lose millions of dollars due to DDoS attacks if they are unavailable for hours at a time. To use the DDoS tools, one does not need to be technically proficient. As a result, DDoS are becoming harder to detect and easy to launch.

In order to understand the trend of assault methods that attackers employ to begin an attack, we examined a variety of DDoS attacking tools in this article. The several defense strategies against these attacks are identified in this paper, which is very helpful.

Service and common in the online community. DISTRIBUTED DENIAL OF SERVICE (DDOS)

The goal of this attack is to prevent authorized users from accessing the resources by flooding the infected devices that are being used by the affected servers with packets. Most of the time, the hosts that are impacted are used by attackers without their owners' knowledge. Sometimes, instead of totally shutting down the service, attackers only want to overload the web servers with traffic in an attempt to harm the system. Therefore, the primary reason for worry at the moment regarding the protection of online systems is DDoS assaults. A DDoS assault consists of four main parts: a victim, zombies, controllers, and attackers. The attack is executed in phases, as Figure 1 shows.. In order to assault the target computer with a denial-of-service attack, the attacker hacks many hosts. In addition to utilizing the single source

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203048 |

computer to assault the target, the attacker utilizes remote authentication to manage all compromised devices and instructs them to submit several requests simultaneously, therefore exhausting the target machine's bandwidth and resources. The handler in this process employs a number of agents, or daemons, to make a number of requests at one certain moment. Attackers overburden the host or router they target, rendering them incapable of delivering services.

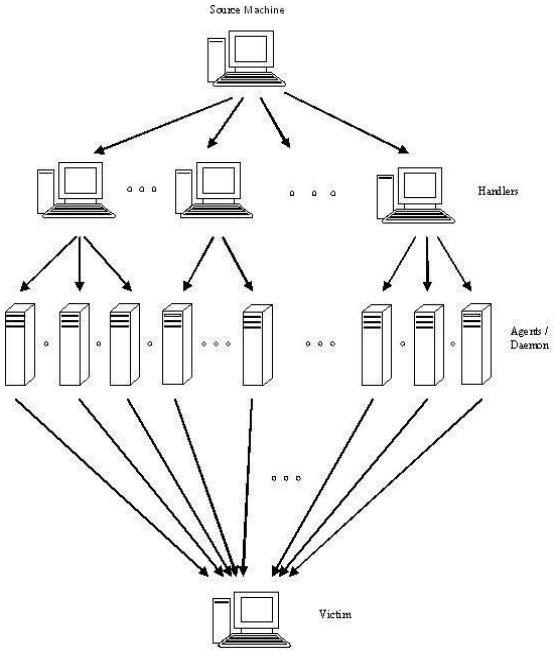

Fig.1. Architecture Diagram of DDoS [2]

III. KINDS OF DDoS ATTACK

Direct and reflector attacks are the two categories within which DDoS attacks fall. While infected hosts make requests with a fake IP address—that is, the target machine's IP address appears in the source address field of IP packets—in reflector attacks, direct assaults involve compromised hosts attacking the target directly.

A. Direct Attacks

In a direct attack, the attacker sends a large number of packets directly to the target, overwhelming it (see Fig. 2). The Attack packets may be in the form of UDP or ICMP or TCP, or a mix of these. A number of strategies, including ICMP flooding, RST flooding, and SYN flooding, were used to carry out the attack. Table I offers a concise overview of the methods.

IP traceback is an additional factor. IP tracebacking is the method of determining the original sender of a packet via the Internet without relying on the packet's source information. Direct assaults allow for IP traceback, however DDoS attacks do not allow for it. This can be carried out following the execution of the attack.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203048 |

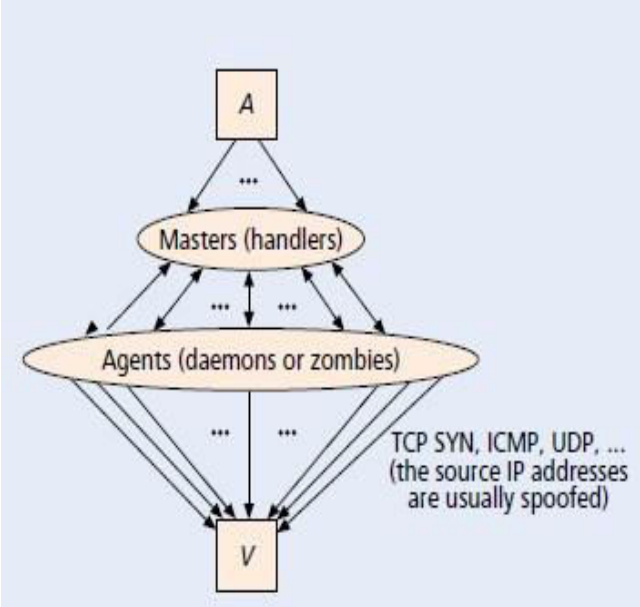

Fig.2. Architecture of Direct Attacks [12]

B. Reflector Attacks

Reflector attacks are carried out by utilizing mediator-like routers, which are designed specifically to serve as attack launchers (see Fig. 3). Reflector attacks can be carried out using the same techniques as direct attacks, but they follow a different approach. Table I provides a brief explanation of these approaches.

Because reflector attacks use spoofing to deliver packets to the target machine through reflectors, the traceback technique is rendered ineffective in these situations. Stopping the attacker from delivering attack packets is a complicated task, even if the attacker is successfully discovered.

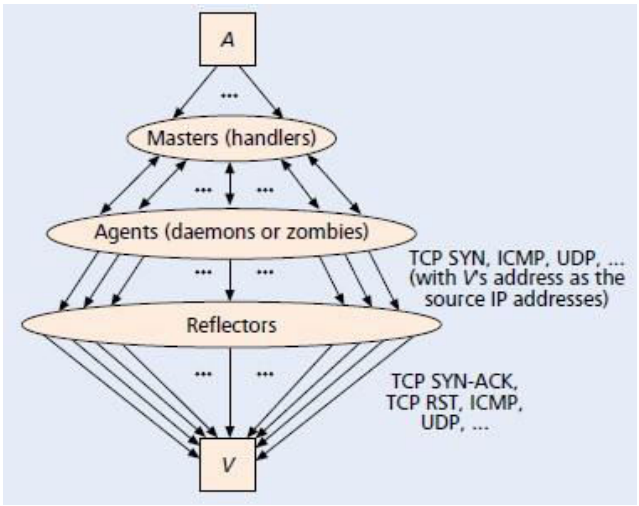

Fig.3. Architecture Diagram of Reflector Attacks [13]

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203048 |

C. Methodologies

TABLE I. DIFFERENCE BETWEEN DIRECT VS REFLECTOR ATTACK

TYPE / METHOD	DIRECT ATTACK [12]	REFLECTOR ATTACK [13]
Method 1: SYN Flooding	A significant amount of TCP SYN packets are sent to the victim's active port during this type of flooding. In the event that the port is continuously open to connection requests, the victim will acknowledge the request by sending SYN-ACK packets back. However, these reply packets are transmitted somewhere else in cyberspace since the attack packets employ fake addresses as their source addresses. Consequently, the victim transmits the SYN-ACK packets a great deal more than once. The victim won't be able to accept any more requests when these quickly deplete all of the resources.	The attacker uses the victim's IP address as the source address in the TCP packet to send TCP SYN packets to the TCP servers, causing the reflector to transmit the TCP SYN-ACK packets in reaction to the intended computer.
Method 2 : RST Flooding	One aspect of RST flooding is blocking the victim's entry point. to compel the victim to reply with RST packets.	The reflector transmits TCP RST messages to the victim and sends TCP packets to non-listening TCP ports.
Method 3:	Most commonly used packet types are UDP and ICMP. In this, the victim responds back by producing the appropriate UDP and ICMP packet response.	The attacker sends the reflector ICMP queries, which are often echo queries, and the reflector replies to the victim with ICMP responses, which are also typically echo answers.

IV. DDOS ATTACKS AND ITS TOOLS

The most widely used tools are examined and contrasted in this study. DDoS attacks can occur in both wireless and conventional networks.. Many various tools or approaches are used to scan susceptible and infected workstations, Nevertheless, only few DDoS techniques are able to reach the crucial stage. Among the most popular DDoS tools are Mstream., Trin00, Low Orbit Ion Canon (LOIC), Tribal Flood Network (TFN), and Trinity. The architectures, channel encryption techniques, and distribution strategies employed by these products vary. To gain a better knowledge of these techniques that will be useful in the future to safeguard the vulnerable systems, we compared the different methods in Table 2 based on the type of flooding, the architecture employed, and the channel encryption.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203048 |

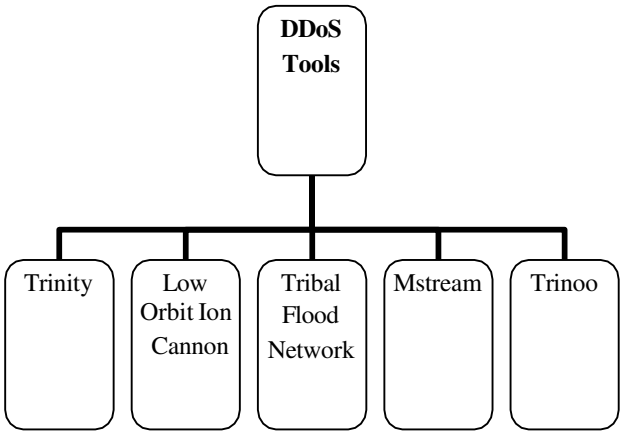

Fig. 4

TABLE 2. COMPARISON AND ANALIZATION OF DDOS TOOLS.

TOOLS / TERMS	TFN [3]	TRINOO [6]	MSTREAM [4]	LOIC [8]	TRINITY [5]
Definitions	TFN is a DDoS tool that attacks the victim's website using TCP SYN flood, Smurf attack, and UDP flood.. To launch a DDoS assault, TFN linked the intruder and the automated program using the CMD interface between agents and handlers or attackers and handlers instead of encrypting communications.	Trinoo is a bandwidth-saving technique that may be used to target one or more IP addresses by using UDP flooding.. The utility uses the target computer's open ports to transmit fixed-sized UDP packets. IP source address spoofing is supported by a previous version of trin00.	The Mstream utility attacks the target host by faking its IP address. For example, attacking the victim's website using fake TCP acknowledge packets. The Mstream utility employs TCP ACK floods, which might overwhelm the data used by switches' routing algorithms in response.	The Low Orbit Ion Cannon (LOIC) is a freely downloadable attack tool for the victim's website. LOIC launches a DDoS assault employing different flooding techniques, such as TCP, UDP, and ICMP, to harm the compromised host's resources, including CPU time, storage, and bandwidth.	Trinity is a tool that floods UDP, TCP, SYN, and TCP acknowledge packets in an attempt to compromise the website. It also offers several new flooding techniques, including as The victim's website is being attacked using TCP fragment, TCP RESET packet, and transmission control protocol random flag packet flooding tactics.
Utilizing architecture	Agents -oriented.	Agents -oriented.	Agents -oriented.	Agents -oriented.	IRCs-oriented.
Flooding technique applied to launch an assault	Direct broadcasting, TCP, ICMP echo request, and UDP echo request	UDP echo	SYN , ICMP and TCP	TCP SYN, UDP, ICMP	UDP, TCP SYN, ICMP
Kinds of DDoS attack employed	Straight approach	Straight approach	Straight approach	Straight approach	Straight approach

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203048 |

Potential harm incurred	Depletion of resources and bandwidth	Depletion of bandwidth and exploitation of remote buffer overflow	Depletion of Bandwidth	Depletion of Resources and Bandwidth	Depletion of Resources and Bandwidth
Encrypting channels	Using the CAST-256 technique, the attacker and handlers' communication channel is encrypted.	Password protection and encryption are also options for communication channels.	Not every communication is encrypted.	The use of encryption in communication	Not every communication is encrypted.

V. CONCLUSION AND FUTURE SCOPE

The number of people using the internet is growing with time. The internet has spread to locations where people would never have imagined that a network of kind, capable of providing access to any kind of information, could exist. Due to the rise in internet usage, many hackers are keeping a watch out for opportunities to conduct assaults in order to obtain vital information or even bring down entire systems. On the Internet, there are several weak systems that might be leveraged to launch DDoS attacks. Furthermore, DDoS attacks will continue to be a potent kind of attack despite the use of protection mechanisms, making them extremely tough to counter. In this paper, we provide a detailed introduction to DDoS, with tabular explanations of the various forms of attacks. We also offer an overview of a few popular DDoS attack tools. Because these tools are automated, even a novice user can utilize them without any technical understanding. Future developments may involve different defenses against DDoS assaults that are launched by different tools that are discussed 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. Dittrich, “The Tribe Flood Network Distributed Denial of Service attack tool”, University of Washington, October 21, 1999.
4. 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. Rocky K. C. Chang, “Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial”, *IEEE Communications Magazine*, pp. 42-51, October 2002.
12. 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.pd f.
13. 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

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details