Distributed Denial of Service Attacks and Prevention Techniques

Mr. Vishal Ramakrishna Powar[1], Ms. Pooja Subhash Naik[2]

[1]Student, Department of Master of computer Application, Finolex Academy of Management and Technology, Maharashtra, India.
[2]Student, Department of Master of computer Application, Finolex Academy of Management and Technology, Maharashtra, India.

---***---

Abstract - *As we are living in the 21 century where the internet is the main factor and security plays a vital role in it.*

Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by sending a large volume of requests from multiple resources.

In this paper we mainly focus on DDoS attacks, and its types, and to find out best prevention and finally, we will conclude the optimum solution for DDos attack

Keywords: *DDoS attacks*, Attacker, Victim

1. INTRODUCTION

The internet in simple language is defined as an interconnected system of networks and can be used to communicate through large or small distances, share information from any place in the world, and access information or answer to almost any question instantly.

As there are various boons, there is a wide range of disadvantages for the same.

As the need for the internet is rising with time, various questions related to its safety comes insight. The reason for internet insecurity is chiefly its design because the foremost concern was its functionality rather than its security and as it is easily accessible to everyone hence.

1.1 DDoS

A distributed denial-of-service (DDoS) attack is a spiteful effort to disrupt regular traffic of a fixed server service with an overflow of Internet traffic.

DDoS attacks accomplish efficiency by utilizing multiple compromised computer systems as sources of attack traffic. Machines can contain computers and other networked resources such as IoT devices.

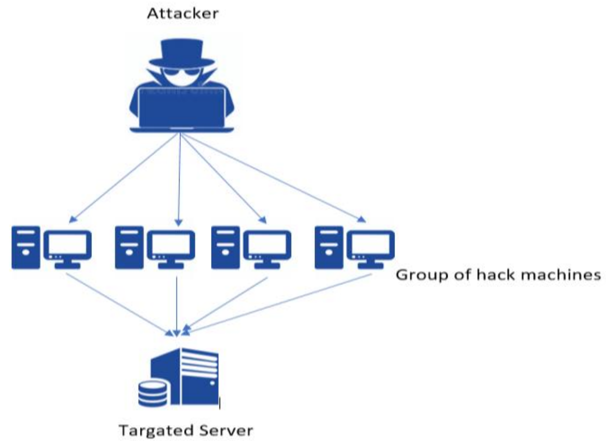
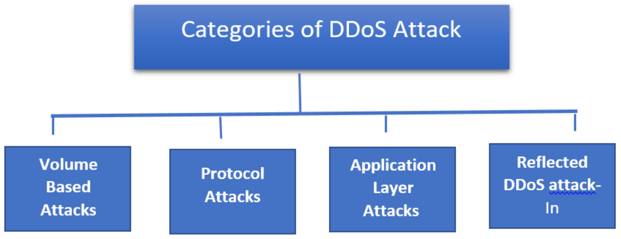


Fig -1: DDos Attack

1.2 DDos Attack



1.1.1 Volume Based Attacks (Bandwidth depletion):

This attacker tries to occupy all the bandwidth of the victim by flooding the traffic using an excess amount of unwanted data (Sometimes 100s of Gbps).

The attacker uses computers and systems all over the world (distributed) to send data packets to the target the victim's bandwidth to get fully occupied, and the server becomes unresponsive. This includes ICMP floods, spoofed-packet floods, and UDP floods. The magnitude measured in a bit per second.

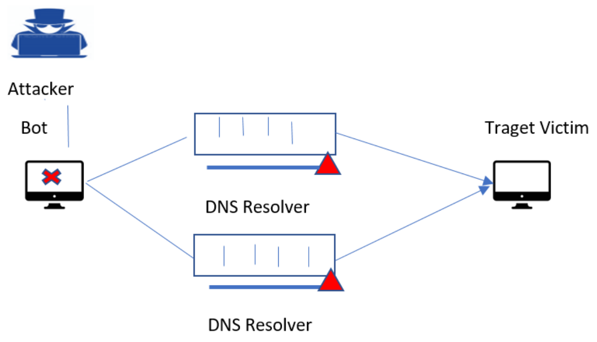


Fig -1: Example of Volume base attack

1.1.2 Protocol Attacks (Resource Depletion):

Instead of targeting bandwidth, the attacker exhausts server resources, this attacker tries to consume all resources provided by the victim, using a large amount of continuous packet sending. They also know the intermediate communication equipment and target them, like firewalls, load-balancer, etc.

This includes SYN floods, death of ping, smurf DDoS, fragmented packets. Magnitude measured in the packet per second.

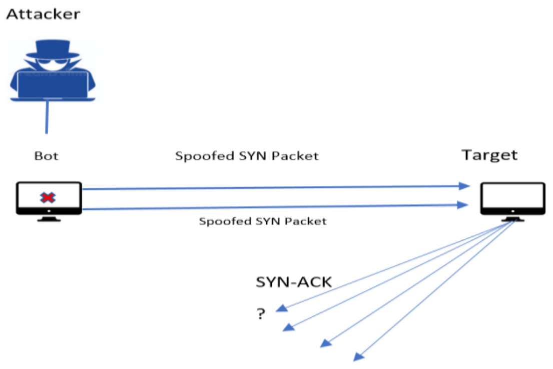


Fig -1: Example of Volume base attack

1.1.3 Application Layer Attacks

This attacker tries to take down victim services by sending higher OSI layer requests such as HTTP GET/POST, and occupy all the memory of the victim server, so this needs lesser resources than others, and it uses specific applications to send requests so that they never get noticed.

This covers a low-and-slow attack, GET/POST floods, then an attack that intends apache, windows liabilities Magnitude is measured in needs per second.

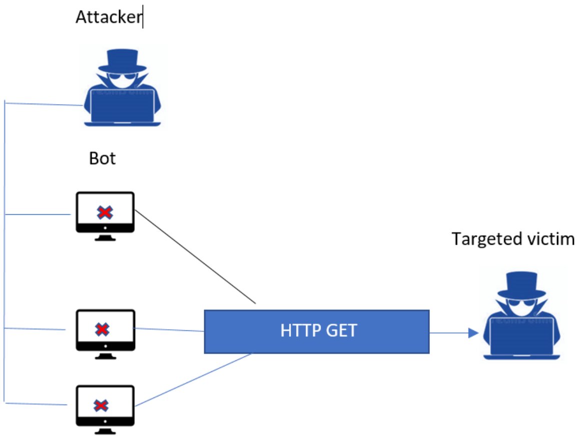


Fig -3: Example of application layer attack

1.1.4 Reflected DDoS attack:

In this case, the attacker sends packets to legitimate third-party servers with the source address of the victim IP, the third-party servers are surely not compromised. This makes lots of response & acknowledgement packets to victims and victims systems get down.

These third-party servers are known as reflectors, and hence attack known as reflector attack. As the attacker is directly not involved in the attack it is very difficult to track back and find the attacker.

Below discuss several prevention methods for fighting DDoS attacks.

1.2 DDoS avoidance techniques

These attacks target data, applications, and infrastructure at the same time to increase the chances of success. To battle them, you need DDoS avoidance techniques.

1.2.1 Rate Limit

Rate limit is the ability of a server or application to restrict the traffic flow to a certain limit, based upon characteristics such as connection per second, packets per second, types-of-queries. The basic idea is to maintain the flow of traffic so that the server can handle requests efficiently.

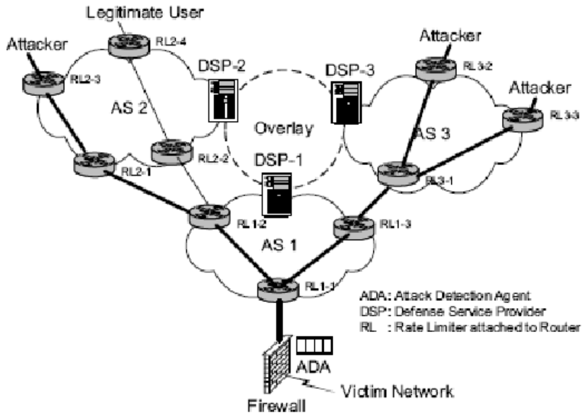


Fig-Rate Limit

1.2.2 Push-Back Approach

This is a method of Rate Limit, additionally this uses the Aggregate-congestion-control (ACC) approach proposed by Mahajan et. al. ACC is a router-based collaborative technique, 'Aggregate' in this context is a subset of traffic with similar properties, such as IP packets with a bad checksum, TCP SYN packets, spoofed packets.

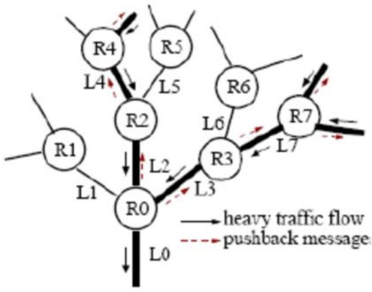


Fig –Push-Back Approach

1.2.3 IP Traceback

Strayer et. al. proposes the architecture for multi-stage traceback to handle DDoS attacks called STARLITE (Stealthy Tracing Attackers Research Light TracE). This is an extension of the Source Path Isolation Engine (SPIE). This architecture works on single package traceback with stepping stone detection

1.2.4 Honeypot

A honeypot is a safety mechanism that produces a virtual trap to trap attackers. This creates an intentionally fake system that allows attackers to compromise services as the original. From that, you can study attack patterns, damage, signs, prevention, and recovery, and apply appropriate security services to original resources. Honeypot can help the security team to investigate and collect data about cybercriminals.

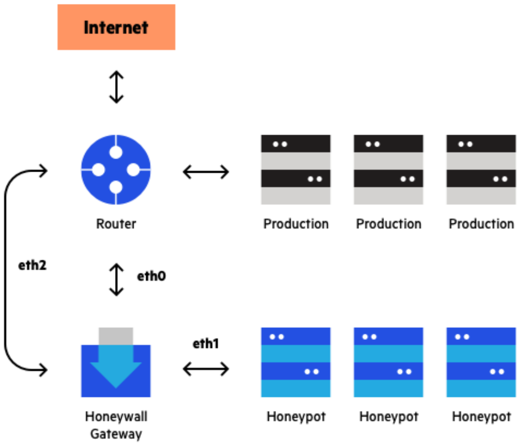


Fig-Honeypot topology

1.2.4 Load Balancing

Load balancing is a DDoS prevention technique that spreads traffic load among several servers so that no single server gets crashed.

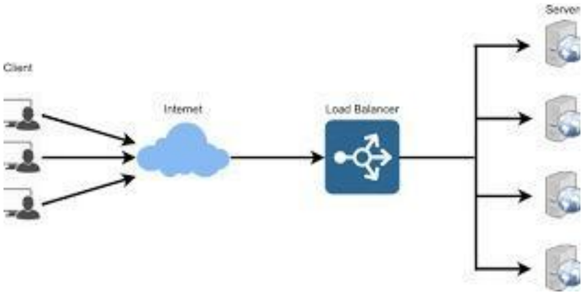


Fig-Load Balancing in network

1.3. CONCLUSIONS

In the current world of networking DDos attack builds huge challenges to researchers, although all the methods, techniques, and mitigations are not possible to discuss so that we have categorized the attack and made the prevention scope limited for this paper. All the discussed preventions have their drawbacks, but they are providing services in various areas, so it is very hard to define the best solution among them. So we have left the scope of this paper to just categorize the solutions.

REFERENCES

[1] Mukhopadhyay, Debajyoti & Oh, Byung-Jun & Shim, Sang-Heon & Kim, Young-Chon. (2010). A Study on Recent Approaches in Handling DDoS Attacks. M. Young, the Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] Mahajan, Ratul & Bellovin, Steven & Floyd, Sally & Ioannidis, John & Paxson, Vern & Shenker, Scott. (2001). Controlling High Bandwidth Aggregates in the

Network (Extended Version). (A later version is in CCR.).

[3] https://www.imperva.com/learn/application-security/honeypot-honeynet/

[4] https://hackernoon.com/what-is-load-balancers-and-how-does-it-work-ep1jr3zcw

BIOGRAPHIES

Vishal Ramakrishna Powar
Student, Department of MCA,
FAMT, Ratnagiri, Maharashtra,
India.

Pooja Subhash Naik
Student, Department of MCA,
FAMT, Ratnagiri, Maharashtra,
India.