A SURVEY ON DENIAL OF SERVICE, DISTRIBUTED DENIAL OF SERVICE ATTACKS WITH POSSIBLE SECURITY MECHANISM

[1]T.Narmadha, [2]Dr.J.Gowrishankar
[1]Assistant Professor, [2]Associate professor
[1]Department of Computer Science and Engineering
[1]Vinayaka Mission's Kirupananda Variyar Engineering College,
[2]Knowledge Institute of Technology, Salem, India

Abstract- Network security is an organization's strategy and provisions for making certain the safety of its assets and every one on network traffic. The first and foremost factor of each network is planning, building, and its operation with powerful security policy. It has become a lot of vital for private pc users, organizations, and the military. There is a large amount of security mechanisms required for different category like personal, commercial, military, and government information. A denial-of-service (DoS) is any kind of attack wherever the attackers (hackers) arrange to stop legitimate users from accessing the service .In a DoS attack, the assaulter typically sends excessive messages asking the network or server to demonstrate requests that have invalid come back addresses. Distributed denial-of-service is one quite the foremost highlighted and most important attacks of today's cyber-world with simple but terribly powerful attack mechanisms. It introduces a huge threat to current web community. In this paper, we are trying to study Denial-of-service attack and Distributed Denial-of-service attack along with various different kinds of security mechanism, techniques, symptoms, Counter Measures and protection tools that can be applied over the architecture of the networks.

Index Terms **- A Denial-of-service attack, DOS, DDOS**

I. INTRODUCTION

A Denial-of-service attack (DOS) is an attack performed on a networking structure to disable a server from serving its clients. The actual intent and impact of DoS attacks are to prevent or impair the legitimate use of a computer or network resources. Moreover, DoS attacks target the network bandwidth or connectivity.

Bandwidth attacks: It overflows the network with a high volume of traffic using existing network resources, thus depriving legitimate users of these resources.

Connectivity attacks: It overflows the system with a huge number of connection requests, thus consuming all available OS resources making it non-responsive for legitimate user requests.

For example: Consider a company (Victim Company) that delivers pizza upon receiving a telephone order. The entire business depends on telephone orders from customers. Assume that a person intends to disrupt the daily business of this company. If this person came up with a way to keep the company's telephone lines engaged in order to deny access to legitimate customers, which would be a revenue loss for the Victim Company.

DoS attacks are similar to the situation described here, where the objective of the attacker is not to steal any information from the target; rather it is to render its services useless.

II .DISTRIBUTED DENIAL OF SERVICE ATTACKS

As defined by the World Wide Web Security: "A Distributed Denial-of-Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the offender is ready to multiply the effectiveness of the denial-of-service considerably by harnessing the resources of multiple unwitting supporter computers and that function attack platforms.

During a DDOS attack, the attacker initiates the attack by sending a command to the zombie agents (infected systems), then these zombie agents send a connection request to a genuine server. These requests sent by the zombie agents seem to be sent by the victim rather than the zombies. Thus, the genuine server sends the requested information to the victim, where the victim machine gets flooded with unsolicited responses from several computers at once. This might either scale back the performance or may cause the victim machine to finish off.

III SYMPTOMS OF A DOS ATTACK

Based on the victim machine, the symptoms of a DoS attack may vary. There are four main symptoms of a DoS attack. They are:

- Unavailability of a particular website
- Inability to access any website
- Historic increase in the number of spam emails received
- Unusually slow network performance

IV DOS ATTACK TECHNIQUES

There are seven kinds of techniques that are used by the attacker to perform DOS attacks as described below:

1. **Bandwidth Attacks:** A bandwidth attack floods a network with a large volume of malicious packets in order to overwhelm the network bandwidth. Here the aim of a bandwidth attack is to consume network bandwidth of the targeted network to such an extent that it starts dropping packets, which may include legitimate users requests.

2. **Service Request Floods:** Service request floods work based on the connections per second principle. Here the servers are flooded with a high rate of connections from a valid source. In this attack, a group of zombies attempts to exhaust server resources by setting up and tearing down TCP connections. e.g., an attacker may use his or her zombie army to fetch the home page from a target web server repeatedly thus resulting load on the server makes it sluggish.

3. **SYN Flooding Attacks:** SYN attack is a simple form of DOS attack, where an attacker sends a series of unlimited fake TCP SYN requests to the victim machine, for which it responds back with an SYN-ACK and waits for the ACK to complete the session, but it will never get the response as the source addresses are fake, as a result the server becomes inactive for legitimate SYN requests.

4. **ICMP Flood Attacks:** A DDoS ICMP flood attack occurs when zombies send large volumes of ICMP_ECHO packets to a victim system, where these packets signal the victim's system to reply, and this combination of traffic saturates the bandwidth of the victim's network connection. Once the ICMP threshold is reached, the router rejects further ICMP echo requests from all addresses.

5. **Peer-to-Peer Attacks:** A peer-to-peer attack is one form of DDOS attack where an attacker exploits the flaws found in the network that uses DC++ (Direct connect) protocol, which allows the exchange of files between instant messaging clients, Here the attacker instructs the client of peer- to-peer file sharing hubs to disconnect from their network and connect to victim's website. as a result, these numerous computers would try connecting to the target website, which causes the drop in website performance.

6. **Permanent Denial-of-Service Attacks:** Permanent denial-of-service (PD0S) is also known as plashing. This refers to an attack that damages the system and makes the hardware unusable from its original purpose until it is either replaced or reinstalled. A PD0S attack exploits security flaws .Which allow remote administration on the management interfaces of the victim's hardware such as printers, routers, and other networking hardware.

7. **Application-Level Flood Attacks:** It results in the loss of services for a particular network, such as emails, network resources, a temporary ceasing of applications etc., as the attackers try destroying the programming source code and files in affected systems.

V.DOS/DDOS COUNTERMEASURES:

The strength of associate degree organization's network security is inflated by putt the proper countermeasures at intervals the proper places. Several such countermeasures square measure obtainable for DoS/DDoS attacks.

The following is that the list of countermeasures to be applied against DoS/DDoS attacks:

- Use robust coding mechanisms like WPA2, AES 256, etc. for broadband networks to resist against eavesdropping.
- Ensure that the computer code and protocols used square measure up-to-date and scan the machines completely to find any abnormal behavior.
  - Improved routing protocols square measure fascinating, significantly for the multi-hop WMN.
  - Disable unused and insecure services.
- Block all arriving packets originating from the service ports to dam the traffic from the reflection servers.
  - Update kernel to the most recent unharnessed.
  - Prevent the transmission of the fraudulently addressed packets at the ISP level.
- Implement psychological feature radios within the physical layer to handle the electronic countermeasures and scrambling reasonably attacks.
  - Configure the firewall to deny external net management Message Protocol (ICMP) traffic access.
  - Prevent the utilization of surplus functions like gets, strcpy, etc.
  - Secure the remote administration and property testing.
  - Prevent the come back addresses from being overwritten.
  - Data processed by the wrongdoer ought to be stopped from being dead.

- The network card is that the entrance to the packets. Hence, use an improved network card to handle an outsized range of packets.

VI DOS/DDOS PROTECTION TOOLS

➢ D-Guard Anti-DDoS Firewall: It provides protection against DDOS attacks. Its main options are:

- Protection against SYN, protocol flooding, and alternative sorts of DDoS attacks
- Built-in intrusion hindrance system
- TCP flow management, UDP/ICMP/IGMP packets rate management
- IP blacklist and white-list, artist white-list, and mack Binding
- Compact and comprehensive log file.

➢ In addition to D-Guard Anti-DDoS Firewall, there square measure several tools that supply protection against DoS/DDoS attacks. a couple of tools that supply DoS/DDoS protection square measure listed as follows:

- WANGuard device
- Net Scaler Application Firewall
- DefensePro
- Anti-DDOS Guardian
- DDOS Defend

VII CONCLUSION

In an effort to secure your network, you must attempt to notice the protection weaknesses and take a look at to mend them as these weaknesses give a path for attackers to interrupt into your network. The most aim of a DoS attack is to lower the performance of the target web site or crash it so as to interrupt the business continuity. Denial-of-service attacks square measure simple ways that to bring down a server. The wrongdoer ought not to have an excellent deal of data to conduct them, creating it essential to check for DoS vulnerabilities. Hence it's counseled to own a DoS Attack Penetration Testing wherever A Pen-tester can simulate the actions of the wrongdoer to seek out the protection loopholes and additionally check whether or not your system withstands DDOS (behaves normally) or it gets crashed. DoS Pen Testing determines minimum thresholds for DoS attacks on your system.

REFERENCES:

[1] Bonguet, Adrien , Bellaiche.2017. Martine A Survey of Denial-of Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing. Future Internet, 9, 43.

[2] Dhara Buch, . C. Jinwala. DECEMBER, 2010 Denial of Service Attacks in Wireless Sensor Networks . Institute Of Technology, Nirma University, Ahmedabad – 382 481, 09-11.

[3]Tasnuva Mahjabin, Yang Xiao, Guang Sun . December 13, 2017. A survey of distributed denial-of-service attack, prevention, and mitigation techniques .International Journal of Distributed Sensor Networks.

[4] Monika Malik et al.June 2015. A Review: DoS and DDoS Attacks . International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, pg. 260-26.

[5] https://www.cloudflare.com/

[6] Raj Kumar, P. Arun ; S. Selvakumar. 2009.Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms. IEEE International Advance Computing Conference.

[7] Qiao Yan ; F. Richard Yu ; Qingxiang Gong ; Jianqiang Li. 2015. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. IEEE Communications Surveys & Tutorials (Volume: 18 , Issue: 1 , Firstquarter 2016).

[8] https://pdfs.semanticscholar.org.

[9] Andry Putra Fajar and Tito Waluyo Purboyo. 2018. A Survey Paper of Distributed Denial-of-Service Attack in Software Defined Networking (SDN). International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 1 () pp. 476-482.© Research India Publications.

[10] http://www.ripublication.com.

[11] Lavanya.A .March- 2017.DDoS Attack and Review of Some Traditional and Current Techniques. International Journal of Computer Science and Mobile Computing, Vol.6 Issue.3, pg. 242-249.

[12] https://searchsecurity.techtarget.com.

[13] www.ijarcs.info/index.php/Ijarcs/article.

[14] Bikram Khadka ,Chandana Withana , Abeer Alsadoon ,Amr Elchouemi . 2015 Distributed Denial of Service attack on cloud: Detection and prevention. .Intehttps://ieeexplore.ieee.org rnational Conference and Workshop on Computing and Communication. https://ieeexplore.ieee.org.

[15] https://www.researchgate.ne