International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org || PP. 62-64

A Distributed Denial of Service Attacks

S.Daisy Fathima Mary[1], N.Rajkumar[2]

[1]*(Lecturer,Department of computer science,Thiruvalluvar University College of arts and science / University , Thiruvennainallur)*

[2]*(Lecturer,Department of computer science, Thiruvalluvar University College of arts and science / University , Thiruvennainallur)*

Abstract: *A denial of service attack (Dos) or distributed denial of service attack (DDos) is an attack to make computer resource unavailable to its intended users. Perpetrators of Dos attacks target sites or services hosted on high- profile servers such as banks, credit card payment gateways, and root nameservers and also to CPU resource management. The Dos attacks either crash or flood the services. The attack involves saturating the target machine with external communication requests which cannot respond to legitimate traffic or responds slowly to rendered as unavailable. In this paper we discuss about the types of Dos attacks, its drawbacks and the preventing measures.*

I. Introduction

Denial of Service (DoS) attacks is a kind of attacks against the computers connected to the Internet. DoS attacks exploit bugs in a specific operating system or vulnerabilities in TCP/IP implementation and it is trying to access the resources to which it has no authorization. The goal of DoS attacks is to keep authorized users from accessing resources. The infected computers may crash or disconnect from the Internet. It is not very harmful, because once the crashed computer is restarted everything is track again and it can be disasters in the cases of corporate network or ISP.

II. Literature Review

The DoS attack detection technologies which include network traffic detection and packet content detection are presented. The DDoS based on DDoS is introduced and some DDoS tools are described and the important TCP flood DoS attack theory is discussed [1]

In the paper “DDoS Attacks purposed to place some order into the existing attack and defense mechanisms, so that a better understanding of DDoS attacks can be achieved and subsequently more efficient and effective algorithms, techniques and procedures to combat these attacks may be developed.[2]

The denial of service attack in distributed is a complex threat and this poses a complicated challenge. According to deep study of organization and size, formulated the problem and represent theoretical proofs for the feasibility of the proposed technique of discrimination in theory. [3].

III. Related Work

The DoS attack is the most popular attack in the network security with the development of network and internet. DoS attacks can compromise the availability of wireless networks as such attacks would essentially prevent one or more nodes from accessing or providing specific services. The network attack and network security coexist and there is no absolute network security environment. There are many reasons for the DoS development. Because some attacks can use the DoS to make money, it becomes the tool of making money. There are many methods to implement the DoS attackthe DoS attack principle and some attack methods are introduced and the program for attack and detection are designed.

IV. History Of Denial-Of-Service

A DoS attack on internet-connected systems was started with the Robert Morris worm attack in 1988. In that attack, Morris, a graduate student at MIT, released a self-reproducing piece of malware (a worm) that quickly spread through the global internet and triggered buffer overflows and DOS attacks on affected systems. Mostly research and academic institutions were connected to the internet at the time, but it was estimated that as many as 10% of the 60,000 systems in the U.S. were affected. Damages were estimated to be as high as $100 million, according to the U.S. General Accounting Office, and Morris was successfully prosecuted under the 1986 Computer Fraud and Abuse Act and sentenced to three years' probation.

TYPES OF DOS ATTACKS

There are two types of Dos attacks namely Denial of service (Dos) attack and Distributed denial of service (DDos) attack.

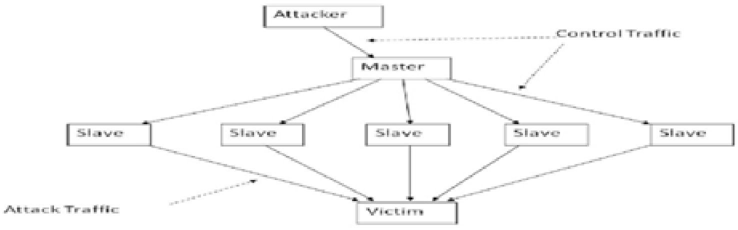
i. Denial Of Service Attack: This type of attack is performed by a single host.The following may indicate such an attack:

□ Degradation in network performance, especially when attempting to open files stored on the network or accessing websites;

□ Inability to reach a particular website;

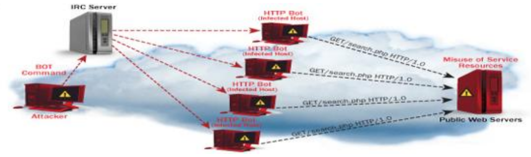
□ Difficulty in accessing any website; and

□ A higher than usual volume of spam email.



DOS Attack

ii. Distributed DoS Attack: This type of attack is performed by a number of compromised machines that all target the same victim. It floods the network with data packets.



In early 2001 a new type of DoS attack became rampant, called a Distributed Denial of Service attack, or DDoS where multiple comprised systems are used to attack a single target. The flood of incoming traffic to the target and it force it to shut down. In a DDoS attack the legitimate requests to the affected system are denied and it is more difficult to detect and block than a DoS attack.

V. Common Denial Of Service Attacks

□ **Ping of Death**

The ping command is usually used to test the availability of a network resource. It works by sending small data packets to the network resource. The ping of death takes advantage of sending data packets above the maximum limit (65,536 bytes) that TCP/IP allows. TCP/IP fragmentation breaks the packets into small chunks that are sent to the server and it can freeze, eboot, or crash.

□ **Smurf**

This type of attack uses large amounts of Internet Control Message Protocol (ICMP) ping traffic target at an Internet Broadcast Address. The reply IP address is spoofed to the intended victim. All the replies are sent to the victim instead of the IP used for the pings. Since a single Internet Broadcast Address can support a maximum of 255 hosts, a smurf attack amplifies a single ping 255 times. The effect of this is slowing down the network to a point where it is impossible to use it.

□ **Buffer overflow**

A buffer is a temporal storage location in RAM that is used to hold data so that the CPU can manipulate it before writing it back to the disc. Buffers have a size limit. This type of attack loads the buffer with more data that it can hold. This causes the buffer to overflow and corrupt the data it holds. An example of a buffer overflow is sending emails with file names that have 256 characters.

□ **Teardrop**

This type of attack uses larger data packets. TCP/IP breaks them into fragments that are assembled on the receiving host. The attacker manipulates the packets as they are sent so that they overlap each other. This can cause the intended victim to crash as it tries to re-assemble the packets.

- **SYN attack**

SYN is a short form for Synchronize. This type of attack takes advantage of the three-way handshake to establish communication using TCP. SYN attack works by flooding the victim with incomplete SYN messages. This causes the victim machine to allocate memory resources that are never used and deny access to legitimate users.

DoS ATTACK TOOLS

The following are some of the tools that can be used to perform DoS attacks.

- Nemesy: This tool can be used to generate random packets. It works on windows.
- Land and LaTierra : This tool can be used for IP spoofing and opening TCP connections.
- Panther- This tool can be used to flood a victim’s network with UDP packets.
- Botnets– These are multitudes of compromised computers on the Internet that can be used to perform a distributed denial of service attack.

VI. Disadvantage Of Dos Attack

Backscatter: It is a side-effect of a spoofed denial-of-service attack. In this kind of attack, the attacker spoofs (or forges) the source address in IP packets sent to the victim. In general, the victim machine cannot distinguish between the spoofed packets and legitimate packets, so the victim responds to the spoofed packets. These response packets are known as backscatter.

If the attacker is spoofing source addresses randomly, the backscatter response packets from the victim will be sent back to random destinations. This effect can be used by network telescopes as indirect evidence of such attacks.

DoS PROTECTION

An organization can adopt the following policy to protect itself against Denial of Service attacks.

- Attacks such as SYN flooding take advantage of bugs in the operating system. Installing security patches can help reduce the chances of such attacks.
- Intrusion detection systems can also be used to identify and even stop illegal activities
- Firewalls can be used to stop simple DoS attacks by blocking all traffic coming from an attacker by identifying his IP.
- Routers can be configured via the Access Control List to limit access to the network and drop suspected illegal traffic.

VII. Conclusion

The best defence is to hinder attackers through vigilant system administration. New services are offered through the internet and new attacks are deployed to prevent clients from accessing these services. If a attack are mainly a network a network problem a solution could derive from alterations in internet protocols. Routers could filter malicious traffic , attackers could not spoof IP address and there would be no drawback in router protocols. If attacks of individual system weakness the solution could derive from an effective IDS system from an antivirus or from an invulnerable firewall.

References

[1]. G. Loukas, and ¨G. Oke, “Protection against denial of service attacks: A survey.” Computer. Journal. 53, pages-1020–1037. 2010.

[2]. J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.

[3]. Barcelona, “Identification of repeated denial of service attacks”, IEEE Communications Society, pp. 1–15, April 2006.

[4]. Aura, T., Nikander, P., and Leiwo, J. “DOS resistant authentication with client puzzles”, Lecture Notes in Computer Science, 2133, 170–177 ,2001.

[5]. Seo, H. S. and Cho, T. H, “Modeling and simulation for detecting a distributed denial of service attack”. Proceedings of Australian Joint Conference on Artificial Intelligence (AI’02), 16-21 September 2002.

[6]. “Detecting distributed denial of service attacks by sharing distributed belief”. Lecture Notes in Computer Science, 2727, 214–225.

[7]. Prof. Pankaj Salunkhe ,Mayur Shishupal,‟ Denial-Of -Service Attack Detection Using KDD,‟ International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 4, Issue 3, March 2015 .