International Journal of Computer & Information Technologies (IJOCIT)
www.ijocit.org & www.ijocit.ir
ISSN = 2345-3877

Preventing from Denial of Service Attacks by Using Multi- Layer Algorithm

Fahime Zarei
Department of information technology
Young Researchers and Elite Club, Kerman Branch, Islamic Azad University, Kerman, Iran
(fahim1592@gmail.com)

Abstract: DOS (Denial of Service) attack is one of the most dangerous attacks to servers. This attack causes the server not to be available anymore and make it shut down. This kind of attack is one of the most unavoidable attacks that are done by using different methods such as Botnet, Zombi. This attack occurs by using a strong server or several altogether the aim server. They do their task (attack) by sending some packet by high speed and high volume. This article helps you to stop this attack by using some ideas on the basis of schedule and information volume. In this method, the multi-layer algorithm is proposed to suppress DOS attacks by any layer are performed. Each layer operations are Performed to suppress DOS attacks.

Keywords: DOS attacks, HTTP protocol, multi- layer algorithm, packet.

1. Introduction

DOS (denial of service) attack is one of the attacks that cause destruction and disorder in resources and services which are being used or accessed. The aggressive server's purpose is to stop the user's system and its connection to internet. In this attack, the aggressive server makes the user busy by sending a large amount of unreal requests and the user can't do the routine and real activities because his system is busy. These unreal requests have a large volume

[1- 3]. The result of this attack is getting down the user's system. This attack is controlled by using various methods like Botnet, Zombi and Dos attacks are divided into six categories: smurf, fraggle, synflood, ping of death, DNS (Domain Name System), land. DOS attack's Technical terms can be divided into two categories: A- service preventing via sending the destructive data that processes these attacks, using the software's objections and faults. (Preventing actions by faults) B- System resources saturations: In this method the aggressive wastes the system resources and the system cannot do its job -which is giving service to its authorized users- well. For example: synflood is one of this kind. However, by updating the software filtering the unwanted traffic, and limiting user's resources, we can overcome these kinds of attacks [4], [8, 9]. Using the counterfeit IP address along the attack, and the appearance of methods of dispensing the attack and some available devices, we can create constant challenges for the users who must overcome the DOS attacks. Since the attack of rebellion of data package tries to depose and destroy the bandwidth resources and processor, the package quantity and the data volume are important factors in determining success rate. In this paper, the multi-layer algorithm is proposed to suppress DOS attacks. This algorithm has several layers that each layer operations are performed to suppress DOS attacks. The rest of the paper is structured as follows: In Section 2, briefly reviews the previous research works deals. In Section 3, related Algorithm for Data Loss. In Section 4, describes the proposed algorithm contains steps and evaluation and finally, In Section 5, includes some conclusions.

2. Literature Review

There is an essential point here that DOS and DDOS(distributed denial of service) attack are the attacks with no certain method to overcome them and the methods mentioned above, are trying to decrease the risks of these attacks [5,6],[10]. Most commonly used methods are as follows:

2.1. Designing and Multiple Supporting

Most of the websites give service to their users on server. These sites are vulnerable because of the danger of server's or router's attacks. But if the sites could run on different servers, the probability of getting offline for these sites would highly decrease. It is undeniable [7]. In ideal situation, in addition to have several connections to the internet, there should be probably geographically long distance between these connections.

2.2. Bandwidth Constraints

If DOS attack is via a single protocol, we can put a bandwidth constraint protocol on its port. For example, if the port number 25 is attacked, it will get busy. Then the other user can't connect to server via number 80. So we can manage this subject or case by using limited policies [17]. Of course if there are several attacks and if the server is attacked by several protocols simultaneously, this limitation can't do anything.

2.3. Starts a Few Services

If there are a few ports on server, there are also a few services, and the risk is less. This technique is called POLP or principle of least privilege.

2.4. Only Necessary Traffic Can Pass On

This defensive method is the same as the previous method. There is only one difference between them. This method can run on network. It means that firewall can only allow necessary traffic pass on. The users always analysis in entrance traffic but it's very important to be external traffic. Necessary filters should run on this external one, for example surveying of network allows all control packets like ICMP(Internet Control Message Protocol) to enter and exit, although it's not essential, what do you think about packets related to ping? Is it necessary to access them completely?

2.5. Use of IP Blocking Policy

This is the most usual and efficient method in confronting DOS. When a site is attacked, we should find the aggressive so we can block it on

central router. The external routers are at the risk of this attack, so the probability of getting successful is little for this policy.

2.6. Use of the Latest Security Packs

We tell all users around the world that security is very important and essential. We know this method can block DOS attacks and other attacks [15]. If there is a new attack, whether DOS or others, the experts start examining the attack and analyzing it, and predict and tell software solutions. These solutions are presented as security packs. After presenting the above methods, they are being compared with DOS preventing methods. These Preventing methods use multi-layer algorithm. Each layer has a function to repress these attacks. These are coordination between these layers completely and there is one end and it is the defeating this attack. Being layered is the distinguish point between this method and the others. None of these solutions have mentioned this kind of preventing. One of the advantages of this method is the ability to repress the attacks from several IPs. It can stop server damage. This method is almost the best one especially to stop botnet.

3. Algorithm for Data Loss

In wireless networks, the connection points of network send the data to the destination and they communicate with each other. However, the destructive nodes defend the nodes which are supposed to be sent to the center [15]. The transmitter sends the data to the needs that act as a destructive factor. The destructive node defends the data. The data is defended because of compression, shortage of energy resources, weak channel conditions as well as destructive actions. We notice the algorithm find the main reason of sending out the data. We have two levels to identify the attacks and list them below:

- ✓ Recognition of the first level:

Transmitter's nodes select controlling node randomly. This controlling node uses the mechanism called watching monitoring mechanism and it controls the process of transferring the data to the next center. If one

node is successfully sent to transfer K, K will be threshold.

- ✓ The recognition of the second level:

The information cross-layer design for the uncertain node from the link layer gained, and for approving the destructive activity of the node in network layer is used. The power of IDS relies on near degree of real reason data downfall. One node can defend the data for many reasons that we mentioned before. The process of data downfall because of one of the above reasons can be introduced as an incorrect action of a node. Therefore, it is very necessary to find and diagnose the best and main reason for data down fall.

4. Malti -Layer Algorithm

The rejecting attacks are being called much, because they are aggressive to computer systems in one single network. DOS attacks usually do their task temporarily. Their task is stopping the network's actions in a period of the time. Service rejecting doesn't let the users use the network. Smurf attacks are the most destructive attacks. They are on the basis of large volume of ICMP packets. The penetrator sends an ICMP (ping) to an area address [11] .the resource address of request is in victim's IP (the victim's IP is used as return address). After receiving echo request, all of the area machines send echo responses to victim's IP address. In this stage, the victim can't do anything because of package rebellion of many machines. This attack uses bandwidth method to disable victim's network and it does its task by using the reinforcement of aggressive bandwidth. In these kinds of attacks, the aggressive sends some information packages (ping) to network broadcast address. The starting address of every information package is replaced by victim's computer address. To stop attacks from available site, the external router should be configured so that all the packages exited with contradictory starting address are obstructed [14], [16]. If the package cannot be falsified cannot get much damage. To avoid exposure as a mediator and co DOS attack another router

configured as Depending on the destination network address, you can block all ICMP packets that the router will not allow the publication of its network [12, 13]. This lets you perform Ping abilities to keep all systems on the network. While allowing the operation of an external system call, to have more safety, we can configure the host systems as we prevent the ICMP currency completely. In this plan, they use several ideas on the basis of time schedule and information volume to prevent DOS. At first step of the algorithm, they have a combination of all the above. At first level, using of one class, they analysis the packages. What pass through this class is some information about this package. The next level involves one class that is created by one single IP. They prepare some reports of all the IP and packages sent. The next step is diagnosing the kind of attack on the basis of reports. This step tells the exact number of packages and their volumes in basic configuration. The last layer or step includes two parts (layers).

4.1. Botnet

Botnet attacks are a set of machines which are related to each other. They are geographically under the control of a hostile power in some situations. Of course the owners of these machines are unaware of these situations. These machines are called Zombi. The software of these BOTNETs has been unsuccessful in confronting aggressive. The word “BOT" from these machines means automatic behavior. They are created and controlled by offender factors and are used to refuse service attacks (DDOS) widely.

4.2. HTTP Protocol

HTTP protocol with many capabilities that despite some limitations, http is one of most qualified protocols used in computer networks (internet, intranet). When a web browser requests a page from the web server, it will actually send an HTTP request to the Web server. A HTTP message can be request or response. HTTP is not related to specific protocol transport layer,

generally uses the TCP protocol (known as port 80).

4.3. Running of Multi-Layer Algorithm

- ✓ The layer of analyzing algorithm of packages on http packets.
- ✓ The middle layer or central layer is for stopping the attack and the change of package's situations.
- ✓ The report layer and returning of information.

5. Conclusion

The essential points mentioned in this research show the most important and applicable methods to overcome some of the attacks. Using the safe accounting, we can't limit in digital rights management. They are used to overcome Botnet. In fiber protective systems that an intelligent user uses to stop rejecting service, this can be used. The basis of a fiber protective system is a modern data structure that is influenced logical fiber. The advantages of this logical system is flexibility, using of logical structure, connected process procedure in global level, local, simple and comprehensive. The presentation of the main copy is being ended, and the results are gained of a separate laboratory. System must be transferred to real conditions. The internal and external filtering is used to encounter the service attacks. According to this filtering, every logical must have an IP address and every other IP is wrong and is the signal of an attack.

References

[1] Agarwal, S., Sommers, J. and Barford, P. "Scalable network path emulation. In *Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)"*, September 2005.

[2] Bianco, A., Birke, R., Bolognesi, D., Finochietto, J., Galante, G., Mellia, M. "Two efficient open-source IP network stacks for software routers". In *IEEE Workshop on High Performance Switching and Routing*, May 2005.

[3] Andersen, D., Mayday, G. "Distributed filtering for internet services". In *Proceedings of USITS*, 2003.

[4] Wagner, Robert. (August 2001). "Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks". Retrieved April 11, 2006.

[5] Bouzida, Y., Mangin, C. "A framework for detecting anomalies in VoIP networks". In: Third international conference on availability, reliability and security (ARES 08) March2008.

[6] Chang RKC. "Defending against flooding-based distributed denial of-service attacks", a tutorial. IEEE Communication Magazine October 2002.

[7] Chen, EY. "Detecting DoS attacks on SIP systems". In: 1st IEEE workshop on VoIP management and security. Vancouver Canada , April 2006.

[8] Dierks, T., Rescorla, E. "The Transport Layer Security (TLS) protocol", version 1.1; April 2006.

[9] Eddy, W. "TCP SYN flooding attacks and common mitigations". August 2007.

[10] lert, S., Wang, C., Magedanz, T., Sisalem, D. "Specification-based denial-of-service detection for SIP Voice-over-IP networks". In: Third international conference on internet monitoring and protection (ICIMP2008). Bucharest, Romania; July 2008.

[11] Geneiatakis, D., Kambourakis, G., Dagiuklas, T., Lambrinoudakis, C., Gritzalis, S. "A framework for detecting malformed messages in SIP networks". In: 14th IEEE workshop on local and metropolitan area networks (LANMAN). Chania, Greece; September 2005. Eid, M., Artail, H., Kayssi, A., Chehab, A. "Trends in mobile agent applications". Journal of Research and Practice in Information Technology 2005.

[12] Bernard, Aboba. IEEE 802.1X Pre-Authentication. Presentation to 802.11WGi, July 2002.

[13] Michael, Lowry, Lough. "A Taxonomy of Computer Attacks with Applications ***to*** Wireless Institute", April 2001.

[14] Bohoris, C., Pavlou, G., Cruickshank, H. "Using mobile agents for network performance management". In: Proceedings of the IEEE/IEFT network operations and management symposium. Hawaii, USA, 2000.

[15] Cheikhrouhou, M., Conti, P., Labetoulle, J., Marcus, K. "Intelligent agents for network management": a fault detection experiment. In: Proceedings of the sixth International symposium on integrated network management, Boston, USA,1999.

[16] Caballero, J., Clamant, S., Barth, A., and Song, D. "Extracting models of security-sensitive operations using string enhanced white-box exploration on binaries", EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-36, Mar 2009.

[17] V. Ganesh and D. Dill, "A decision procedure for bit-vectors and arrays" ,in Proceedings of the Computer Aided Verification Conference, Berlin, Germany,Agust2007.

Authors profile:

Fahime Zarei is M.Sc. student of information technology at University of Qom in Iran. She received her B.Sc. degree in information technology from Kerman University of Iran in 2010. Her research interests are in the fields of: network security, Cloud Computing, programming and related domains.

