Survey on DoS Attack detection: Location Guard and CAPTCHA

Miss. Desai Sucheta¹, Miss. Anushka Pawar²
Miss. Renushe Tejasvita³, Mr. Naik L. S.⁴
¹,²,³,⁴ Department of Computer Engineering,
Rajendra Mane College of Engineering & Technology, Ambav, Devrukh.

Abstract: Denial of service (DoS) attack is one of the major security threats to the software system. The detection of DOS attack is a very important research topic. In DOS attack, the attacker sends a large number of useless packets/requests to the targeted machine by using different resources and this transmission is done in a very short period of time. This process will consume the targeted system's resources as well as making the targeted system's services unavailable. Among all types of network attacks, the DOS attack is a very harmful type of attack. Hence, there is a need to detect and prevent such a harmful type of attack. In this paper, we focus on different possibilities or ways of DOS attack as well as its detection and prevention.

Keywords – Location Guard, Captcha, Attack tools.

1. INTRODUCTION
DOS attacks basically target websites like banks, payment gateways. In Denial of Service attack, the attacker sends the flood of fake requests to targeted clients. Hence the target machine remains busy with hostile clients (attackers) and cannot communicate with authorized clients. When the flood of requests exceeds the buffer capacity of the targeted machine, the DOS attack happens. In this paper, we propose the method to detect the DOS attack which comes under Intrusion Detection System. We also propose the location guard method and refer the Captcha to prevent the DOS attack. We will provide the mathematical Captcha in login form on our website. The legal users enter into the website by filling the login form as well as solving the mathematical Captcha. Each time the Captcha comes in different shapes and patterns. Normally we verify Captcha submitted by users before allowing access to the system. The attacker will enter into the website without solving the mathematical Captcha but this illegal activity of
attacker gives clue that unauthorized person is entered into system. This activity of attacker is called as abnormal behavior or abnormal activity and when such abnormal activity is occurred in system then the system triggers an alarm. Therefore that activity is flagged and logged as abnormal. Hence in this way we can detect as well as prevent the DOS attack.

2. MODULES:-

2.1 Location Guard

The Location Guard receives the request from the client. Then it processes that request. This location guard is used in between the client and the file server. If any user enters in system without submitting CAPTCHA then location guard identifies that users are unauthorized. Therefore the location guard should not allow that unauthorized user to access the system hence that users are automatically discarded.

3. ATTACKING TOOL:-

The DOS attack get spread in system easily because of availability of already built attacking tools. These tools are very powerful therefore they can easily generate attacking traffic. Following are attacking tools which we will use to implement DOS attack:

3.1 TFN :

By using this attacking tool the communication between attacker and targeted client is produced by command line interface. The data communication between targeted machine and attacker is in unencrypted format and that communication is done via ICMP echo reply packets. By using this attacking tool we will implement the IP Flood or Synchronization flood types of attack.

4. ATTACK TYPE:-

In our project we are going to implement one of the following types of Denial of Service Attack:

1. IP Flooding
2. Synchronization Flooding
4.1 IP Flooding:

IP Flooding is a type of Denial of Service attack where the attacker sends the large number of requests to the targeted machine. Hence the system is flooded with fake IP addresses. Therefore, it will be resulted in IP flooding type of DOS attack.

4.2 Synchronization flooding:

In Synchronization flooding type of attack the attacker repeatedly send synchronization packets to the targeted machine using fake IP addresses. In this type of attack the acknowledgement is never return back to the target machine. The attacker sends multiple SYN [5] requests to targeted machine. Hence, targeted machine remains completely busy to responding each SYN request. Therefore, that machine should not communicate with authorized clients.

5. DETECTION:-

5.1 Anomaly Based Intrusion Detection System

We are going to use the Anomaly Based Intrusion Detection technique to detect the DOS attack. Because it is trusted technique and it will detect any new type of attack. This technique focuses on behavior of the system. When any abnormal activity is arises in system then anomaly based IDS [6] technique should triggers an alarm. Hence, that abnormal activity will be discarded.

6. PREVENTION:-

6.1 CAPTCHA [3]:

CAPTCHA is used for verifying the user. In our project website we are providing the
mathematical CAPTCHA on login page of website. Before login to website the user need to solve the CAPTCHA. We will verify the CAPTCHA submitted by the user and if it is correct then we allowing that user to access the website. The normal user first solves that CAPTCHA and entered into system but attacker will enter into system without solving CAPTCHA. But this abnormal activity of attacker should get detected by anomaly based IDS. Therefore that user will be discarded. Hence DOS attack will also get prevent.

CONCLUSION

DoS attack may block the resources of the targeted system. In this paper, we covered an overview of the DoS problem, available DoS attack tools, defense challenges and principles, and a classification of available DoS prevention mechanism. This provides better understanding of the problem and enables a security administrator to effectively store his data with proper prevention mechanisms for fighting against DoS threat. This paper will give the details of plan and implementation of application which will detects and prevents DOS attack. This will also overcome on various disadvantages found in existing system thus making it more efficient and reliable.

REFERENCES