Survey of Distributed Reflection Denial of Service Attack and Its Detection Techniques

Mr. More Vikas[1], Assistant Prof. Deokate Gajanan[2]

[1] ME Student, Department of Computer Engineering, SP COE, Maharastra , India
[2] Assistant Prof., Department of Computer Engineering, SP COE, Maharastra, India

ABSTRACT

Distributed Reflection Denial of Service is the recent iteration in the series of Denial of Service attacks. It works similar to Distributed Denial of Service, in that it uses many sources to attack one victim and the attacker hides behind the zombies. In this paper, we concentrate on assisting the nodes of network during the DRDoS attack, by using detection algorithm to detect the attack whenever a suspicious flow is noticed and then by proper analysis of the network we can find the attack free path which can be used by the nodes in the network. We use Rank Correlation based Detection algorithm which helps to find whether the network is experiencing a channel failure or is under attack. Once the attack is detected, the attack path and source are multicast to all nodes, so that the nodes in the network can avoid any traffic from them, thus reducing the effect of DRDoS attack for a specified period of time.

Keyword: - *Distributed Reflection Denial-of-Service (DRDoS) attack, Distributed Denial of Service attack, Rank Correlation based Detection, matching algorithm.*

1. Introduction

DRDoS is the next generation of Distributed Denial of Service (DDoS), which uses an ingenious variation on the traditional SYN attack to actually trick innocent servers and core infrastructure routers into unknowingly executing a DDoS attack. DRDoS uses legitimate hosts called "reflectors" to flood the victim by making slaves spoof the victim's address. A reflector may be any IP host that will respond to other request messages, like SYN, SYN/ACK, ICMP request, DNS queries and so on.

The procedure of DRDoS attack is briefed in Figure 1. It works as follows: An attacker first controls some zombies and locates a large number of reflectors. Then it sends attack commands to zombies. When received attack commands, the zombies send request packets with victim's address to the reflectors. That is, zombies send Request with Source: victim and Destination: Reflector. And reflector, based on the forged source addresses in those Request packets will send Response with Source:Reflector and Destination:Victim. At last, victim is flooded by the numerous unsolicited response packets from the reflectors adding up to significant bandwidth, enough to congest the victim's Internet connectivity. With bandwidth maxed out, legitimate clients are not able to connect with the victim

2. LITERATURE SURVEY

2.1 A System for Denial-of-Service Attack detection based on Multivariate Correlation Analysis [1]

Multivariate correlation analysis algorithm for detection of denial of service, Interconnected systems, such as Web servers, database servers, cloud computing servers etc, are now under threads from network attackers. A DoS attack detection system is proposed that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features.

2.2 Network-based detection systems

Network-based detection systems are loosely coupled with operating systems running on the host machines which they are protecting. Network-based detection systems can be classified into two main categories

Misuse-based detection systems: It detects attacks by monitoring network activities and looking for matches with the existing attack signatures. In spite of having high detection rates to known attacks and low false positive rates, misuse based detection systems are easily evaded by any new attacks and even variants of the existing attacks**.** **Anomaly based detection**: It monitors and flags any network activities presenting significant deviation from legitimate traffic profiles as suspicious objects, anomaly-based detection techniques show more promising in detecting zero-day intrusions that exploit previous unknown system vulnerabilities.

2.3 Analyzing well-known countermeasures against distributed denial of service [5]

Classifies DDoS defense techniques based on defense points defense methods can be classified in four categories:

1. Source-end defense techniques Source-end defense points are the best points to filter or rate-limit malicious traffic because minimum damage occurs for valid traffic.

2. Core-end defense techniques In these techniques any core route independently tries to detect malicious traffic and then filter or rate limit the traffic

3. Victim-end defense techniques Victim-end defense points can easily separate DoS traffic from valid traffic. The major problem with victim-end defense techniques is that victim-end defense points are not good points for rate-limiting or filtering attack traffic because the bandwidth might be saturated

4. Distributed defense techniques Source-end points are promising points to rate-limit or filter malicious traffic; core-end points are promising points to only rate-limit traffic regardless of type of traffic and finally victim-end points are promising points to detect and discriminate DoS traffic from valid traffic. So, a cooperative mechanism between source-end and victim-end, or between core-end and victim-end, or between source end, core-end and victim-end can be favorite defense techniques against DDoS attacks.

2.4 Fuzzy based technique [7]

Fuzzy is a software tool to test the end user application and protocols. Each time there is a situation to implement a new protocol or software or any application. It must be tested with fuzzy tools. The tool will decide whether it can be implemented in real-time and it weather it is a secure one or not [7]. Filter based approach: Flow level filter is used to detect the low rate DDoS attack. Low rate DDoS attack which gradually increase the traffic rate and attack the network host. Flow level filter which blocks the DDoS attacks [1] [8].

2.5 Types of DoS attacks [7]

The Different types of Dos attacks are as follows

1 Smurf Attack

This attack floods the victim’s bandwidth. In this method, the attacker sends a large number of ICMP echo requests. Hence all the ICMP messages have spoofed source address as that of victim’s IP address. This attack floods the victim’s bandwidth.

2 Syn Flood

SYN Flood attack is the most popular and effective brute force DoS attack. SYN Flood attack sends TCP connect request with SYN flag to the victim server. Then the victim server returns ACK acknowledgement to the attacker, but the attacker doesn't acknowledge, so the connection is not established fully, and this kind of connection is called half connection. The victim server maintains a huge number of half-connections which will cost a mass of resources.

3 Router HTTP Attack

The router HTTP attack is a kind of semantic attack. If the Cisco router has not set the "not HTTP server" rule, the attacker may lock the router until the administrator reboot the router by sending the HTTP request like "GET /000 HTTP/1.0" to the router. At the beginning of the attack, the attacker needs to probe the router's web service port and status. If the web server is running, the attack can continue. Then the attack data need to be constructed, and socket need to be open. These two steps are both the precondition of sending the request, and they can be executed in parallel.

4 Reflected/Spoofed Attack

A Distributed Reflected Denial of Service attack (DRDoS) involves sending forged requests of some type to a very large number of computers that will reply to the requests. Using IP address spoofing, the source address is set to that of the targeted victim, which means all the replies will go and flood the target. ICMP Echo Request attacks (Smurf Attack) can be considered one form of reflected attack, as the flooding host sends Echo Requests to the broadcast addresses of the misconfigured networks; thereby many hosts send Echo Reply packets to the victim

5 Slow Read Attack

Slow Read attack sends legitimate application layer requests but reads responses very slowly, trying to exhaust the server's connection pool. Slow reading is achieved by setting a very small number for the TCP Receive Window size and at the same time by emptying clients TCP receive buffer slowly. With this action we have a very low data flow rate.

3. CONCLUSION

DRDoS attacks are a growing problem. The main question is “How do we know if we are under attack”? The option we have covered has its pros and cons. The Solution concentrates on detecting DRDoS independent of specific protocols using the Rank Correlation based Detection algorithm. We also suggest some methods to reduce the disadvantages of DRDoS by identifying the path causing the attack and avoiding the path to send packets for a specified time period. There are a lot of interesting works in the future, including: 1) Extend the experiment against real DRDoS in the Internet. 2) The algorithms can be used in more complicated network scenario which uses many routers. 3) Include tracing methods to find the attacker for better avoidance of the attack.

6. REFERENCES

[1]. Wei Wei, Feng Chen, Yingjie Xia, and Guang Jin “A Rank Correlation Based Detection against Distributed Reflection DoS Attacks”, IEEE Communications Letters, Vol. 17, no. 1, January 2013.

[2]. Lei Zhang, Shui Yu, Di Wu and Paul Watters “A Survey on Latest Botnet Attack and Defense”, 2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11.

[3]. Vern Paxson, “An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks”, Computer Communication Review 31(3), July 2001.

[4]. Tao Peng, Christopher, Leckie Kotagiri Ramamohanarao, “Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring”, In Proceedings of the Third International IFIP-TC6 Networking Conference(2002).

[5]. Yonghui Li, Yulong Wang, Fangchun Yang, Sen Su , “Traceback DRDoS Attacks”, Journal of Information & Computational Science 8: 1 (2011) 94–111

[6]. T. Hiroshi, O. Kohei, and Y. Atsunori, “Detecting DRDoS attacks by a simple response packet confirmation mechanism,” Computer Commun., vol. 31, no. 14, pp. 3299–3306, 2008.

[7]. T. Vogt, “Application-level reflection attacks.” Available: http://www.lemuria.org/security/application-drdos.html

[8]. Divya Bansal, Sanjeev Sofat, “Use of cross layer interactions for detecting denial of service attacks in WMN”,2010

[9]. S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, “Discriminating DDoS attacks from flash crowds using flow correlation coefficient,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 6, pp. 1073–1080, 2012.