RESEARCH ARTICLE OPEN ACCESS

Study on Recent Trends of Distributed Denial of Service Attack and Handling Approach

Rajnish Kumar Mishra [1], Amarnath Singh [2], Vipin Kumar Gupta [3]
Cyber Laws and Information Security Division
Indian Institute of Information Technology
Allahabad - India

ABSTRACT
This research paper explains the techniques and trends of an attacker to execute distributed denial of service (DDoS) attack to any targeted system based on recent incidents on various ISPs. DDoS attacks are newly evolved attack which actually attacks on the availability of the services and resources of the targeted system. A normal DDoS can be executed from anywhere in the distributed network and chock the victims service or server by sending large number of packets. Few countermeasures have been given by many researchers in this field. There are various technical experts and researchers are still working on this issue which became a very big problem for every service provider organization but still we do not have such solution to overcome with this problem completely .In this research paper we have introduced the attackers trend to perform DDoS in these days which is reflection based DDoS attack and their proposed mechanisms or methods to overcome with this problem up to the acceptable table.
Keywords:- DDS Attack, MTN

I. INTRODUCTION

In today's internet environment we are mostly dependent on the technological things .we are accessing the services and information within a second through the internet connectivity where security is main concern which derives the concept of CIA: Confidentiality, Integrity, Availability. There are many security threats associated with each but recently, new type of security threats have emerged: one, which does not target the integrity or confidentiality of resources, but rather their availability. This newly evolved threat is known as Denial of Services (DoS) Attacks .DoS attack is an attack which prevents authorized users to use specific network service or resource such as any website, web service, or any system's resource .There are many incidents related to DDoS which happened in past and recent past like Indian telecom regulator TRAI's website was down due to DDoS attack and many organization has been suffered from DDoS attack like MTN and GitHub.so this is emerging and highly severe attack by which many organizations are suffering .many E-Commerce websites are getting slow down due to DDoS attack performed by the attackers .Attackers are following many ways to perform DDoS attack on their targeted system but In these days mostly attackers are following reflection based DDoS attack which is new trends of the attackers to perform DDoS attack .

In this paper we will explain the reflection based DDoS and amplification based DDoS attack. There are four section in this paper, In the first section we will be discussing reflective DDoS and amplificative DDoS attack ,second section will be based on the DNS reflection attack because to perform reflection based attacks the attackers are using many resolvers and DNS is one of them which are using by the attackers to perform DDoS attacks and section third will be the few countermeasures of DDoS attack proposed by the researchers ,fourth section describes the conclusion of the discussion about the whole paper .

1.1 REFLECTION BASED ATTACK

Recently DDoS related incidents was performed by the attackers which was Reflection based .To perform reflection based attack the attackers are

using **spoofed IP address** of the target on which they want to perform DDoS attack. The attackers are following this trend and using many reflectors to perform reflection based DDoS attacks. Few most common reflectors are as follows which are being used in this type of attacks. [3]

A. DNS Server (Open Resolver Type)
B. NTP Server
C. Gaming Server
D. Chargen Protocol
E. SNMP Server etc.

Out of the above reflectors we will discuss about DNS reflector only because it is very difficult to discuss about every reflectors and how they are being used by the attackers to perform DDoS attack so we have kept our scope limited to DNS as reflector only and we will be discussing in the second that how DNS Servers are being used to perform DDoS attacks.

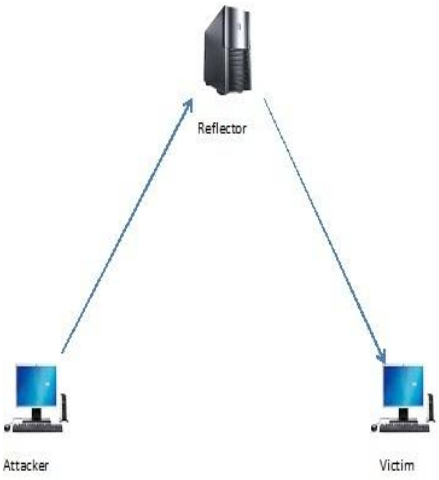

FIGURE-1 REFLECTION BASED DDoS ATTACK

1.2: AMPLIFICATION BASED ATTACK

Amplification based DDoS attack is same as reflection based attack but in this attack the response rate of the reflectors get amplified .This is done by the attackers to get large volume of response at the victims side by sending multiple request query to multiple reflectors and multiple reflectors responses to that query so those multiple responses will go to the victims system which will be in large amount and DDoS will occur.

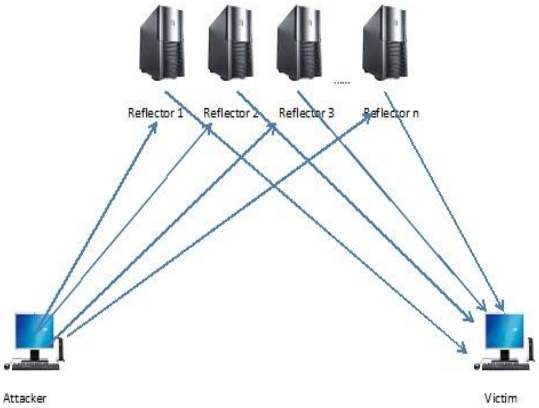

FIGURE-2 AMPLIFICATION BASED DDoS ATTACK

Figure-2 Amplificative DDoS Attack

II. DNS REFLEXTION AND AMPLIFICATION BASED DDoS ATTACK

DNS is domain name system which translates a domain name in to the IP address and provides response with the information needed according to request query [4]. Now in these days attackers are using DNS server which is open resolver type DNS to perform DDoS attack .Open resolver type DNS server can do the recursive query to its top level domain name system (DNS) and process the request of any user or client .So attackers are taking the advantage of this property of open resolver type DNS and perform the DDoS attack to any victim. To perform the DNS reflection based DDoS, attackers performs the following task. [5]

a. Spoof the IP Address of the target or victim
b. Send request query to DNS (open resolver) server by putting the spoofed address of the target or victim.

DNS will receive that request from the attacker, process the request and sends the response to spoofed address which is present in the packet of the request. So here response is reflecting to the victim's end which will disrupt the service of the victim and DDoS will occur.

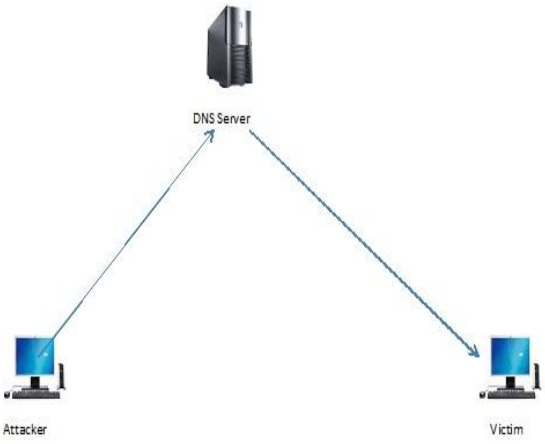

FIGURE-3 DNS REFLECTION ATTACK

Figure-3 DNS Reflection Attack

In DNS amplification attack, same thing will happened but here attacker sends multiple queries to the multiple DNS Server by putting the same spoofed IP Address in the request. DNS server contains various records and based on the request DNS responds with information to victim. This makes the response size bigger at the victim's end which will disrupt the victim's services. Response size of DNS is much bigger than request size so here multiple responses will be sends by multiple DNS servers to the victims system and DDoS will occur.

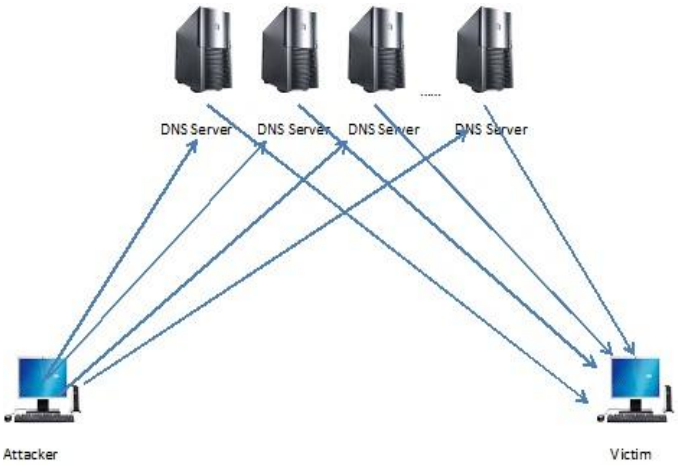

FIGURE-4 DNS AMPLIFICATION ATTACK

Figure-4 DNS Amplification Attack

III. COUNTER MEASURES OF DDoS

There are many mechanisms and models have been proposed by various researchers to overcome with this type of attack but it is difficult to discuss each and every mechanism or method recommended by various researchers over here .So in this paper we discuss few techniques to avoid DDoS attack which are as follows.

a. Rate Limiting
b. BCP 38

3.1 RATE LIMITING

The Experts and researchers have done a lot of work in reference to the counter measures the DDoS with the use of a mechanism called as Rate Limit framework. But, in this paper we discuss the model explained by **Jing ET AL**. Mr. Jing's model follows the following three processes.

[1]. Detecting the Attack

[2]. deciding the Rate limit

[3]. Applying the Rate limit to all attack traffic

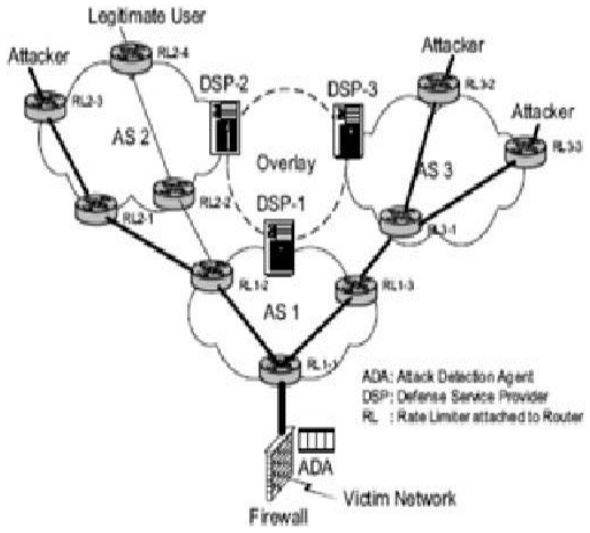

Figure-5 Architecture O2 DN

The above model is O^2 -DN architecture with three major modules which is as follows

1. ADA – Attack Detection Agent

2. DSP- Defense Service Provider

3. RL - Rate Limiter

Here above architecture shows that ADA can be placed at the victim's network or firewall which will be responsible for generating alert if any attack is detected and sending the query to DSP for every detected attack .ADA can be a software or a hardware which is users choice to install software or implement hardware .DSP receives the defense query from ADA and goes to the Rate Limiting decisions .After taking decision it sends few instructions to RL which is related to rate limit. Here RL provides rate limit of the traffic flow given by ADA. Installation of RL is done by ISP and managing the RL is the task of DSP in same domain.

3.2 BCP 38

BCP 38 is best current practices 38 which belongs to a RFC 2827 .This is recommended to every service provider to implement BCP 38 to mitigate DDoS .Generally In DDoS attack ,attacker uses spoofed IP addresses so BCP 38 implementation mitigates the IP spoofing by ingress filtering in the network .If any user will send the spoofed IP address request then network ingress filter will Identify that address and if that address belongs to the same network then it allows otherwise drops the packet .This is shown in figure -6.[7]

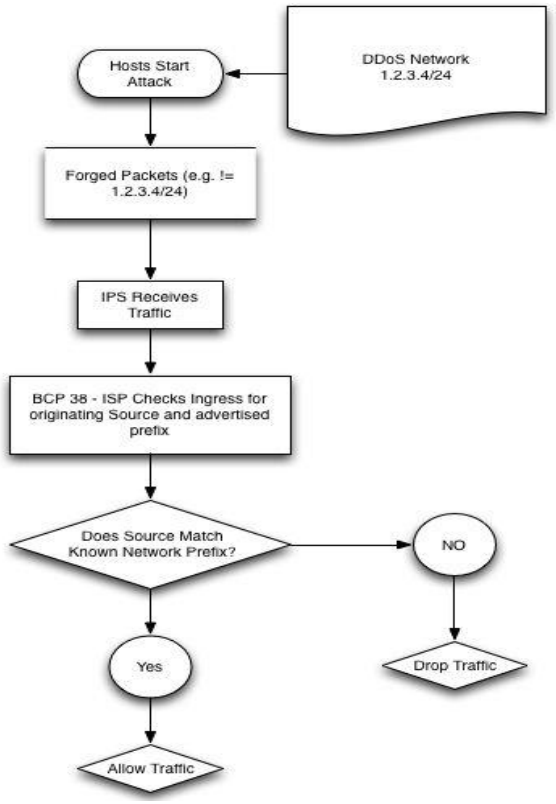

Figure-6 BCP 38 Working

Apart from above measures of DDoS there are others like Active filtering and Response handling which can play an important role in counter measure the DDoS attacks.

IV. CONCLUSIONS

Distributed Denial of Service (DDoS) attack is now became a great challenge for the various ISP's (Internet Service Providers) as well as researchers who are working in the field of network security in the word. To handle this great challenge a lot of research and work have been done and based on that

a lot of recommended models and mechanisms are there. In this research paper we have discussed two major methods that are being considered by the experts in network security area. Although it is very difficult and impossible to present each and every published task and propose the ultimate solution because still many researchers and technical experts are doing efforts on this challenging attack. So we have explained only two major methods in this paper.

REFERENCES

[1] https://www.us-cert.gov/ncas/tips/ST04-015

[2] https://threatpost.com/arbor-ddos-attacks-getting-bigger-as-reflection-increases/108752\

[3] http://www.prolexic.com/kcresources/white-paper/white-paper-snmp-ntp-chargen-reflection-attacks-drdos/An_Analysis_of_DrDoS_SNMP-NTP-CHARGEN_Reflection_Attacks_White_Paper_A4_042913.pdf

[4] https://www.nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdf

[5] http://referaat.cs.utwente.nl/conference/19/paper/7409/detecting-reflection-attacks-in-dns-flows.pdf

[6] http://www.redbarn.org/dns/ratelimits

[7] https://isc.sans.edu/forums/diary/DDoS+and+BCP+38/17735/