International Journal of Scientific Research in Computer Science, Engineering and Information Technology

© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

DDOS Attacks and Possible Countermeasures : A Review

Archana Tulsiyani[*], Ekta Singh, Prof. Chandresh Parikh

Department of IT & Telecommunication, Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT

The exceptional success & growth of internet has changed many traditional services such as banking, educational, groceries, shopping and many more. Now they are progressively working towards the safe and fast process. The present era, can be said as the era of the internet as the world is highly dependent on the internet which can be considered as the main infrastructure for the growth of global information society. Therefore, the availability of the internet is the perilous for social & economic growth of society. However traditional architecture of the internet is vulnerable which therefore provides the window of opportunity to the lots of the attack. Distributed denial of service (DDoS) attack is one of those attacks, which poses an enormous threat to the availability of the internet. The cloud milieu has many security challenges among which DDoS attacks have maximum priority. Within Cloud Security issues being dominant for the private enterprises, the denial of service attacks is rated as the highest priority threat. One of the immense bother before the researchers is to find the details of attack as many organization avoid to revel that they were attack due to the frighten of the defamation. DDoS exhaust victim's bandwidth on service. In this paper an overview of distributed-denial-of-service, different types of attack, different types of techniques, and their countermeasures are reviewed.

Keywords: Availability, DOS, DDOS, Attack, Security.

I. INTRODUCTION

Cloud computing is a strong aspirant to folk IT implementations as it offers low-cost and "pay-as-you-go" based access to computing capabilities and services on demand. Many organizations are shifting their IT structure into the cloud. Infrastructure clouds commits oodles of benefits over fixed infrastructure. These advantages include "pay-as-you-go", avaibility of data whenever required and much more. Whereas, there are various questions in mind about cloud which is discussed in literature [4][5]. The "availability" means the information should be accessible all the time. Threat to the internet availability is a big issue which keep one's nose to the grindstone to the growth and survival of e-business & other products. Internet like another product is vulnerable to failure. Internet failures can be accidental or deliberated. The design of the internet mainly focuses on providing functionality. Therefore, it provides little attention on designing the damage control from the accidental failures. On the other hand, deliberated attack done by the malicious insider/hacker/cracker have no answer to the original design of Internet. Security issues associated to the cloud computing are applicable to various participants for an informed cloud adoption decision. Apart from data breaches, the cyber security community is frequently visiting the attack space for cloud-relevant solutions as these issues has influence on budget, resource management, and service quality. A Denial-of-Service (DoS) attack is an attack that prevents the legitimate users from accessing the services. DoS attacks manages this by sending huge amount of information that triggers a crash. Some common DoS attacks are SYN-ATTACK, TEARDROP, SMURF, FINGER BOMB, BLACK HOLE etc. Distributed Denial of Service (DDoS) attacks degrade or completely interrupt services to legitimate users by expending communication and/or computational resources of the target. DDOS attacks are escalated form of DoS attack, where the attackers direct hundreds or even thousands of compromised hosts known as zombies against one sole target. These zombie hosts are unwittingly recruited from the millions of unprotected computers accessing the Internet through high-bandwidth and always available connections.

There are five types of dos attacks are mentioned. In network device level attacks, the target is some device on network. The attack is launched by exploiting some software bug or hardware resource vulnerability. In Operating System (OS) level attacks, vulnerabilities of operating system in the victim machine are used to launch dos attack. In application level attacks, bugs or vulnerabilities in the application are identified to exploit them for dos attack. Port scanning for identifying open ports of a remote application is very common in this perspective. Such attacks are now getting more widespread as they present the traffic to a network and its devices similar to the licit traffic. Therefore, in a scenario where most of other attacks are now identifiable, application level attacks offer more success rate to attackers [6]. Heavy traffic is generated by the attacker towards the victim to dissipate connectivity or bandwidth resources so that normal services are denied or degraded for requests of licit users. In protocol attacks, the vulnerability of some protocol features is used to exploit them for launching a dos attack. For example, the source IP address of a data packet. There are various types of DDoS attacks as classified in [1][2]. However, the most common form of the DDoS attack is called packet flooding attack, in which large number of purportedly legitimate TCP, User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) packets are directed to specific destination. As per Peng [3] defending against these type of attacks is challenging for two main reasons. First, the number of zombies involved in a DDoS attack in a very large topographical area. The volume of traffic sent by single zombie might be inundate. Secondly zombie usually spoof their IP's under the control of the attacker, which makes it very difficult to traceback even the zombies.

II. OVERVIEW OF DDOS

The Operating System and network protocol are not evolved by keeping security as centre point which in result provides number of unpatched and unsecured machine on the internet as a result they are used by hacker for performing their activities. These unsecured and unpatched machines are used as a main source of the DDoS attacker as their army of *bots/zombie* for attack. These *bots/zombies* are the vulnerabilities for the public network as hackers can attack these types of system and inject the malicious code or using any other technique they take control over these types of machines and are then added to the army of their *bots/zombie*. These malicious machines can be in hundreds or thousands of numbers. They all behave like an agent of the attacker. The network of these type of malicious machine is known as the "**Zombie network**". The size of the zombie will define the magnitude of the attack. For example: If the number of the *zombies/bots* are in large number then the impact of the attack is severe. The following figure 3 shows how the DDoS attack works. Within the "Botnet" or "Zombie network" chooses the "HANDLER" which controls and command the *bots*. The *bots* attack directly to the victim. There are group of the agents (*bots*) under each "Handler". These "Handlers" is the medium of communication between "*bots" &* "Master". It also passes the information of the victim got from the "*bots"*. As the "handler" and "zombie" are also compromised machines in the public network under the control of an attacker, the users of these machines are unknown to the fact that they are used as part of the botnet network. A typical architecture of DDoS attack is mentioned below

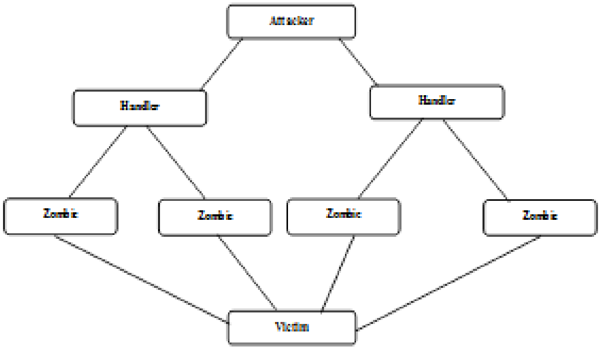

Figure 1. Architecture of Bortnet

III. CLASSIFICATION OF DDOS [14]

DDoS Attacks is considered one of the major attack that create havoc on the network as well as applications. For ease of understanding and development of various tools DDoS attacks has been classified into 3 types:

3.1 Volume Based Attacks:

Considered as one of the most common attack techniques used for launching DDoS attacks. The main modus operandi of volume based attacks is the saturation of the bandwidth of the victim's site or network by applying various techniques. This prohibits the legitimate users to access the site or the network, thus rendering the services useless to the users. Leads to the server crash. The major techniques used for launching volume based attacks are UDP floods, ICMP floods and other spoofed attack floods. The magnitude of volume based attacks is measured upon bits-per-seconds. In 2016, it was observed that there was around 650 Gbps DDoS floods of more than 150 million packets per second(Mpps).

3.2 Protocol Based Attacks:

Protocol based attacks consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers. These attacks mainly focuses on exploits of the vulnerabilities of layer 3 and 4 of OSI model. The magnitude of protocol based attacks is measured in packets per second (Pps).They are also known as state-exhaustion attacks. Some of the common known attacks are SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS.

3.3 Application Based Attacks:

Application based attacks are generally considered as most devastating as it is rather harder to identify a DDoS attacks is happening. Also known as Layer 7 DDoS attack. A single HTTP request is cheap to execute on the client side, and can be expensive for the target server to respond to as the server often must load multiple files and run database queries in order to create a web page [15]. Types of Application based attacks are Http flood attacks based attacks. Attack traffic is usually legitimate, targeting the application layer and involves triggering a back-end process that blocks the resources and making it temporarily unavailable. For this reason, these types of attacks are comparatively harder to detect and prevent. In a survey, the number of attacks in quarter 4 of business reached an all-time high, with an average of 889 application layer assaults per week.

IV. EXISTING SYSTEM

A number of different attack tools or “stressors” are available for free on the Internet. The basic usage of some of these tools are considered to be legitimate as security researchers and network engineers may at times perform stress tests against their own networks to understand the havoc created after an actual attack. Some attack tools are specialized and only focus on a particular area of a particular layer of the protocol stack, while others will be designed to allow for multiple attack vectors to target multiple layer at the same time. *Attack tools can be broadly characterized into several groups:*

Low and slow attack tools

As the name implies, these types of attack tools both use a low volume of data and operate very slowly. Designed to send small amounts of data across multiple connections in order to keep ports on a targeted server open as long as possible, these tools continue to utilize server resources until a targeted server is unable to maintain additional connections. Uniquely, low and slow attacks may at times be effective even when not using a distributed system such as a botnet and are commonly used by a single machine.

Application layer (L7) attack tools

These tools target layer 7 of the OSI model, where Internet-based requests such as HTTP occur. Using a type of HTTP flood attack to overwhelm a target with HTTP GET and POST requests, a malicious actor can launch attack traffic that is difficult to distinguish from normal requests made by actual visitors.

Protocol and transport layer (L3/L4) attack tools

Going further down the protocol stack, these tools utilize protocols like UDP to send large volumes of traffic to a targeted server, such as during a UDP flood. While often ineffective individually, these attacks are typically found in the form of DDoS attacks where the benefit of additional attacking machines increases the effect.

A few commonly used tools include:

Low Orbit Ion Cannon (LOIC)

The LOIC is an open-source stress testing application. It allows for both TCP and UDP protocol layer attacks to be carried out using a user-friendly WYSIWYG interface. Due to the popularity of the original tool, derivatives have been created that allow attacks to be launched using a web browser.

High Orbit Ion Cannon (HOIC)

This attack tool was created to replace the LOIC by expanding its capabilities and adding customizations. By utilizing the HTTP protocol, the HOIC is able to launch targeted attacks that are difficult to mitigate.

The software is designed to have a minimum of 50 people working together in a coordinated attack effort.

Slowloris

Apart from being a slow-moving primate, Slowloris is an application designed to instigate a low and slow attack on a targeted server. The elegance of Slowloris is the limited amount of resources it needs to consume in order to create a damaging effect.

R.U.D.Y (R-U-Dead-Yet)

This is another low and slow attack tool designed to allow the user to easily launch attacks using a simple point-and-click interface. By opening multiple HTTP POST requests and then keeping those connections open as long as possible, the attack aims to slowly overwhelm the targeted server.

V. DDOS INCIDENT

Due to current trends of the industry to provide increasing bandwidth for the better availability of services it has provided the attackers to launch a large-scale DDoS attacks. The main reasons behind any DDOS attack can be financial, non-financial or distraction from actual source. There are many DDOS attacks toolkits that made it quite easy to launch a small level of DDoS attacks. The toolkits are extremely sophisticated, easy-to-use and powerful, thus helping in increasing the opportunity to launch such DDoS attacks. DDOS attacking programs are made up of very simple logic structures and are small in size, thus, making it easy to embedded in any other codes or programs. Various DDoS attacks against high-profile websites such as Yahoo, CNN Amazon and E Trade in early 2000, series of attacks on grc.com in May, 2001 [8] and mydoom virus attack on SCO website in Feb. 2003 demonstrate how devastating DDoS attacks are and how defenceless the Internet is under such attacks [9]. Because of DDoS attacks, the services of these websites can become unavailable for hours or even days. This can cause huge financial losses to all the businesses relying on internet could earn a huge financial loss. Real DoS incidents in the Internet between the years 1989 and 1995 were investigated in [10]. The three most typical effects were the following: 51% of these incidents filled a disk, 33% of the incidents degraded network service, and 26% of the incidents deleted some critical files. A single incident was able to cause several types of damages at the same time (the sum of percentages is more than 100%). [9] The Domain Name System (DNS) is a continuous target for DoS attacks and still considered one of the major application related DDoS attacks. In October, 2002, all root name servers experienced an exceptionally intensive DoS attack. Some DNS requests were not able to reach a root name server due to congestion caused by the DoS attack. Another major DoS attack was launched on June 15, 2004 against name servers on Akamai's Content Distribution Network(CDN), which blocked nearly all access to many sites for more than two hours. One recent attack on the servers of Dyn, which is currently controlling most of the internet's DNS infrastructure. It happened on 21st October, 2016 and remained under sustained assault for the most of the day, bringing down sites including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US.

VI. DDOS DETECTION & MITIGATION [14]

After reviewing the papers related to DDoS attacks and its classification, many detection parameters needed careful study to understand the pattern. The ability to detect precisely the cases of false positive and false negative in a system that is under DDoS based attacks requires considerable accuracy and reliability, which help to reduce such types of attacks on the system. It is also seen that accurate detection and mitigation of DDoS based attacks is considered challenging, as the traffic are in huge amount at the network hops and thus, difficult to distinguish between normal data and traffic data. For DDoS mitigation, effective detection of the type or volume of the DDoS attacks should be implemented. The main purpose of 'DDoS mitigation' to prevent the target machines or systems from any type of DDoS attacks. Basically, for effective detection the mitigation process is divided into 4 stages:

1. Detection: The identification of the type of traffic flowing deviations which could cause or lead to a DDoS attack.

The best detection method is considered to be as early as possible detection of DDoS attacks.

2. Diversion: Traffic is diverted from the target in order to either filter it or discard it.

3. Filtering: DDoS traffic is removed only after clearly identifying the patterns that helps to differentiate between legitimate traffic and malicious attackers. Quick Response is the method to quickly block the attack and not interrupting the user experiences of the visitors.

4.Analysis: Security logs are studied and researched to gather information about the attack, in order to identify the attacker and plan the future improvements to security of the system. Detailed security logs could provide exclusive details about the attack.

VII. FUTURE WORK

DDoS Attack tools are available plenty in the market, which are generally open-source and can be used with few efforts. But the same is not true with the detection & prevention tool. DDoS attack prevention tools or software are too costly to be implemented by small vendors, business or educational institutes. So, the future proposed work consists of a tool that is easily available & used by the small corporate business and educational institutes that helps to mitigate the deadliest DDoS attack.

VIII. CONCLUSION

In this review paper, we presented a review of Distributed-Denial-of-service-attack along with the possible countermeasures in cloud environment. Attacks based on Network layer and Application layer are reviewed. In this we have tried to give the insight of the DDoS Attack by including the Overview of DDoS, Classification, Motivation of DDoS Attacks & its problem along with the recent DDoS incidents.

IX. REFERENCES

[1]. Douligeris C.and Mitrokotsa A.,"DDoS Attacks and Defense Mechanisms: Classification and State of the Art," Computer Journal Of Networks,vol.44,no.5,pp.643-666,2004.

[2]. Mirkovic J.and Reiher P.,"A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," Computer Journal of ACM SIGCOMM,vol.34,no.2,pp.39-53,2004.

[3]. Peng T.,Leckie C.,and Ramamohanarao K.,"Survey of Network Based Defense Mechanisms Countering the DoS and DDoS Problems,"Computer Journal of ACM Computing Surveys,vol.39,no.1,pp.123-128,2007.

[4]. B.R.Kandukuri,V.R.Paturi,A.Rakshit,Cloud security issues,in: Services Computing,2009.SCC ’09.IEEE International Conference on,2009,pp.517–520,doi: 10.1109/SCC.2009.84 .

[5]. L.M.Kaufman,can public-cloud security meet its unique challenges? IEEE Se-cur Priv 4 (8)(2010)55–57.

[6]. Nilesh A.Suryawanshi S.R.Todmal DDoS Attacks Detection of Application Layer for Web Services using Information based Metrics International Journal of Computer Applications (0975-8887)Volume 117-No.9,May 2015

[7]. Gaurav Somania,M.S.(30 march 2017).DDoS Attacks in Cloud Computing: Issues,Taxonomy,and Future Directions. Elsevier,19.

[8]. Gibson S.,"The Strange Tale of the Denial of Service Attacks Against GRC.COM," http://grc.com/dos/grcdos.htm,2007.

[9]. Monica Sachdeva,Gurvinder Singh,Krishna Kumar and Kuldip Singh," DDoS Incidents and their Impact: A Review",The International Arab Journal of Information Technology,Vol.7,No.1,January 2010

[10]. Howard J.,"An Analysis of Security Incidents on the Internet," PhD Dissertation,Carnegie Mellon University,1997 Statics

[11]. K.Santhi Sri,PRSM Lakshmi," DDoS Attacks,Detection Parameters and Mitigation in Cloud Environment",International Journal for Modern Trends in Science and Technology,Volume: 03,Special Issue No: 01,February 2017

[12]. http://www.bcmpedia.org/wiki/Denial_of_Service

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

[14]. www.incapsula.com/blog/650gbps-DDoS-attack-leet-botnet.html

[15]. https://www.cloudflare.com/learning/DDoS/what-is-a-DDoS-attack

[16]. https://blog.thousandeyes.com/how-to-analyze-DDoS-attackf-dns-infrastructure

[17]. Adrien Bonguet and Martine Bellaiche A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defences in Cloud Computing future internet 2017.