RETROACTIVE ANALYSIS OF DENIAL OF SERVICE ATTACKS AS PART OF NETWORK FORENSIC

Ayush Chahuhan, Mitali Chand, Prabhjot Kaur*

Department of Computer Science and Engineering,
Uttaranchal University, Dehradun, India
*Corresponding Author: info.prabh@gmail.com

Abstract: Network forensic deals with the unauthorized invasion identification in a network by recording, capturing and analyzing the network traffic. It is a broader term used to identify and prevent different kinds of network threats and attacks. One such category of network attack is Denial of Service attack (DOS). This paper comprehensively examines the DOS attacks available in various datasets. The DOS attacks such as: Fraggle, smurf, NTP, UDP flood, WinNuke, TCP Syn flood, ICMP flood etc. have been extensively examined. A brief description of tools and techniques used to capture and identify these attacks and accuracy obtained is specified analytically. The authors have also made an attempt to uncover the specifics of the tools used by attackers to launch the aforementioned DOS attacks. Various defense mechanisms have been laid down in order to guard the network against DOS attacks. A framework scenario has been proposed to identify the DOS attack from the legitimate network traffic. The proposed scenario seems to accurately identify the network intrusion to a fair extent.

IndexTerms **– network forensic, DOS, attacks.**

I. INTRODUCTION

The technologies around us are advancing day by day, the advancements in the technologies help us save our time and money and also help us to do certain tasks that we were not able to perform earlier. But as every coin has two sides these advancements in technologies also have negative effects as the technologies are advancing there is also an increasing rate of cybercrimes that are causing certain problems around the globe. There are certain crimes that are occurring over the web, these crimes can be related to hacking, data manipulation, banking, etc. The persons behind these kinds of activities are using certain tools and techniques that enable them to perform these kinds of activities. There are many techniques to hack someone's details and personal information. DoS attacks termed as Denial of Service attacks and DDoS attacks expanded as Distributed denial of service are the most frequently used method to carry out such kind of activities **[9]**.

Denial of service attacks are over the internet for several years now. Previously used single source attacks are easy to tackle and it is easy to protect a system against these kinds of attacks. But as the technologies have advanced to such an extent the attacks are also developed and so many computers became vulnerable to such kind of attacks over the last decade. A denial of service is a cyber-attack in which the person initiating the attack makes a device or network inaccessible to its users. It is done by transitorily or impermanently agitating services of a host associated to the internet. DoS are generally practiced by flooding the target device or network with pseudo requests to overload the system or network and make it inaccessible for the users.

DDoS attacks are being used by the hackers now as the requests that are sent to the target device or network are generated from different sources in this kind of attacks. As the sources are different and are large in number it is difficult to identify the root cause or root source of the attack. Thus making it easy for the hackers not to get exposed. DOS or DDoS attacks are same as a group of people crowding an entry door of any store that makes it difficult for the genuine customers to enter the store **[9]**. Thus, disrupting the trade. Another way of explaing this attack is where the initiator or the attacker use several distinctive IP address, repeatedly there are thousands of them. Since the approaching traffic is originated from many distinctive sources, it becomes nearly absurd to stop these attacks by using the old methods. This even makes it difficult to distinguish the attack traffic and the legitimate user traffic as it is spread along so many point of origins.These attacks can even involve forging of IP addresses i.e. IP address bluffing, which makes it further more difficult to identify and defeating the attacks.The scale of these attacks is countinously rising over the past years, it exceeded a terabit per second in 2016.

These attacks are generally targeted on upraised profile net providers like payment gateways of certain websites, banking servers, government's official websites etc. Revenge, activism and blackmail can give rise to such attacks.It is in records that the elementary DOS attack was manifested by Khan C. Smith in 1997 while an DEF CON function Disrupting the internet access of the Las Vegas Strip for more than one hour. A sample code was released during the function. EarthLink, E-trade, Sprint and other minor as well as major corporations were affected bythe release of DoS attack of over the following years. A DDoS attack was recently encountered on 5thMarch 2018. The attack was targeted on a US based service provider. The attack that took place on 5th March 2018 reached a peak of approximately 1.7 terabites per second and was the bulkiest DDoS attack in the history. DOS as explained earlier makes a device or network inaccessible to its legitimate users. DOS attacks can be categorised in two general forms: attacks which crash the services and attacks which flood services. However the most effective or serious are the distributed attacks.

Layer 7 DDoS attack is the refferal name for application layer DDoS attack. In this type attackers are focused on the application layer. This attack overuses one or more specific functions or features of the target website trying to disable the target functions or features.they are completely variant from a network attacks. It is majorly used contrary to monetary organizations in order to distract IT and also the security members . In 2013 out of all the DDoS attacks 20% attacks were application layer attacks.

Mafiaboy was the first dominant distributed- denial of service attack (DDoS) culpable for disabling some of the internet's most popular websites and was carried out by Canadian citizen Michael Calce on February 2000. On January 2001 register.com encountered the first extensive attack associating DNS servers in the form of reflectors followed by a denial of service attack drifted as factor of a student expedition from NUI Maynooth on The Irish Government's Department of Finance server on February 2001. On October 20, 2002 an attack targeting 13 root name servers used botnet to each server sent huge amount of ICMP ping packets, however the damage was minor s the server were immune with packet filters. Worm Blaster attack was spread on computers running operating systems Windows 2000 and Windows XP crippled 48,000 computers in August 2003. MyDoom attack had two prompt-first it caused the virus to start a denial of service (DoS) attack on Feb. 1, 2004, the next dictated the virus to stop dispersing itself on Feb. 12, 2004.In 2005, a SYN flood was used to drain viable network connections and prohibit users to access to Panix servers. Few Top Level Domain (TLD) and DNS (Domain Name System) root named server operative were subjected to various denial of service (DoS) attacks between December 2005 and March 2006 these attacks actively muck up name resolution service by directing an overpowering quantity of traffic on the communications channels that name server operatives avail to provide service. On April 27 2007 the Estonian government websites were debilitated by a series of DDoS attack and became partially inaccessible. On January 2008, the Church of Scientology website was crippled for several days in New Jersey.

The introduction section summarized the meaning, types and real time incidents of DoS and DDoS attacks. Further sections include the literature review, discussion and conclusion part. In literature review, exhaustive survey of existing DoS attack detection and mitigation techniques used by different researchers is presented thoroughly. The authors also evaluated the importance of methodical survey by inspecting importance of the order and techniques for survey and experimental study **[12, 13]**. The discussion and conclusion part summarizes the details of the attacks studied and their prevention techniques.

II. LITERATURE REVIEW

There are various DoS and DDoS launching attacks methods given by dofferent researchers and one of them is a three way step. The basic steps included in dispatching a DDoS attack are: Discovering the unprotected hosts, Compromise, Communication, and the last launching the attack **[3].**

There are many techniques to overcome from DDoS attacks but the emphasis must be on its prevention techniques. DDoS attacks generally consists of three step line defense modules i.e. traffic monitoring, traffic analysis and traffic filtering and the order of placement of these three modules. DDoS defense as a whole can be implemented in either centralized or distributed way. Centralized defense can itself be vulnerable for DDoS attacks as it itself consumes a large volume of traffic. However, distributed defense is not vulnerable to DDoS attacks as the defense modules are not placed at the same place and hence do not fall prey to DDoS attacks and is able to detect and fight against attacks in a comparatively better way [**4**]. In a real scenario, on February 2000 DDoS took on new visibility, while denial of service attacks disabled the websites of E*Trade, Amazon.com, Buy.com, eBay, Yahoo, Excite, CNN and ZDNet.com,. They submitted various starting points rein into a DDoS attack as these attacks were very bulky **[15]**.

In order to increase the intensity of attacks, the attackers started to arrange compromised computers to networks centrally controlled by IRC "bots." Thousands of compromised computers are manipulated by a single controller is able to manipulate thousands of compromised computers and order them to steal credit card details, send spam email or arise DDoS attacks by the means of "botnets" **[6]**. Labeling the ambushed computers by IP address is the most promising techniques to protect from denial of service attacks. A single botnet could include thousands of computers with randomly distributed IP addresses that is why Botnets invalidated many of these techniques **[15]**.

Al-Jazeera, an Arab satellite television network on March 2003 was uprooted from the Internet and a reason was considered that the attack might have had something related to the war in Iraq led by U.S **[4]**. In the year 2003 Blaster worm also managed to taint exceeding 1.4 million computers across the world **[14].** December 2010 As the DDoS attacks against human right sites and independent were common in 2009 **[10]**.

A survey was conducted among 317 human rights sites and independent media sites shown that 62% of the total sites have experienced a DDoS attack, 32% sites faced defacement, 39% sited experienced intrusion, 72% of the participating sites faced filtering, and 81% sites among the sites who faced DDoS attacks also faced an intrusion, defacement or filtering at least once **[15]**.

A DDoS detection method was introduced by the authors based on Hadoop that in the distributed computing platform implements HTTP GET flooding detection algorithm in MapReduce. MapReduce based detection algorithm is proposed by the authors and the algorithm includes two methods i.e. counter based method and Access pattern based method **[16, 1]**. The authors proposed a DDoS prevention technique using cracking algorithm. The attacker finds one or more system that can be used by them for conducting a DDoS attack. Generally, a system with large number of users is unsafe and thus, meets the attacker's requirements. As the users over the internet are increasing people attempt to attack system resources. By keeping on continuous logon on a particular website for a long period of time the service that is provided by the web server keeps on degrading. To tackle this, this algorithm application keeps a track of the IP addresses of the current users along with their status. When an IP address logs in for the first time it is stated as genuine user, and if the same IP address keeps on logging in for around it is stated as normal user. And as soon as the same IP address logs in for the fifth time its status changes to attacker. After this, the user IP is denied for further services and thus the user cannot get the services on the same IP address. This method of Cracking also includes algorithmic steps which includes packet filtering and MAC generator. Packet filtering inspects the packets that transfers between different computers on the internet. If a certain packet matches the predefined rules of packet filters the packet is straight away dropped by the filter. MAC generator differentiates between the packets having genuine IP addresses and the packets that contain forged IP addresses **[17]**.

One of the reports on DDoS Threat Landscape (2013-2014) showed that among the network DDoS attacks SYN flood attacks having large volume compromises a whooping fraction of 51.5% of the total large-scale attacks **[18]**. Multi vector threats accounts for 81% of the total number of attacks. Among all the multi-vector attacks if SYN flood and large SYN flood attacks are combined they cover about 75% of all the multi-vector attacks. As the attackers are becoming advanced day by day the volume of the attacks is also increasing about 33% of all the attacks were above 20Gbps. The most common large scale attack was NTP reflection attack **[7]**. Among the application layer attacks the DDoS bot traffic saw an increase of about 240%. Among all the botnets present all over the world India, China, and Iran if combined together held about 25% of all the botnets. Among the top 10 DDoS attacking countries USA was ranked 5thmore than 50 targets were attackedby 29% Botnets each month. Around 29.9% of the Bots were able to hold cookies. Among all the spoofed or forged user-agents 46% were fake Baidu Bots while fake Googlebots were only 11.7%.

There have been motivations behind the DDoS attacks such as hacktivism, vigilantism, and attacks that are sponsored by states. The tools used in network traffic collection include such as wireshark, tcpdump, iris etc. and identification of DDoS attacks are available widely **[11, 20, 21]**.

These tools include trinoo, shaft, TFN2K etc. can be used to launch an attack. And defense mechanism against these attacks includes potentially planted accesses, overlay networks, effective monitoring, firewall planted security, refining mechanism etc. As the internet is advancing day by day so are the threats. One of the latest internet service that is becoming popular is cloud computing. As cloud computing is being used all over the world the DDoS attacks saw a major change in the aim of the attacks, targets, methodologies, and scale. The attack bandwidth reached a whooping amount of 500GBPS in 2015 **[5]**. And as the attacks saw a change in the aim after the emergence of cloud computing, this can be seen as 33% of the total attacks that were carried out in 2015 were targeted on cloud services **[2]**. As cloud servers uses various servers that are present all over the world. Thus, it becomes vulnerable to DDoS attacks. These cloud service can be provided security by adopting several techniques such as hiding servers or ports, giving access to selective devices etc. DDoS attacks will be focusing more upon internet services like cloud computing and IOT i.e. Internet of Things because these are the internet services that are emerging and will be used extensively in near future **[22]**.

III. DISCUSSION

In smurf attack, a message is directed to the broadcast the channel via ICMP protocol with bluffed source address. Though there can either be broadcast or normal ping. However, spoofed or bluffed broadcast ping in which victim's channel is flooded with packets of echo nature **[5]**. In Syn flood attack, the vulnerability in three-way of handshake are exploited to occupy usable resources of targeted server and make it unavailable to the intended users **[8]**. In UDP flood attack scenario, the targeted machine is flooded with enormous UDP packets leading to unresponsiveness of the targeted machine towards other nodes. NTP attack is acronym for Network Time Protocol works in synonym with UDP attack in a way of flooding the targeted machine with UDP traffic **[7]**. The WinNuke attack exploits the remote host's vulnerability and the unsaved data on the machine gets lost **[6]**.

Table 3.1 Volume of DDoS attack each year

Year	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Volume of traffic(in Gbps)	0.4	0.4	1.2	2.5	10	17	24	40	49	100	60	60	309	400	500	1100

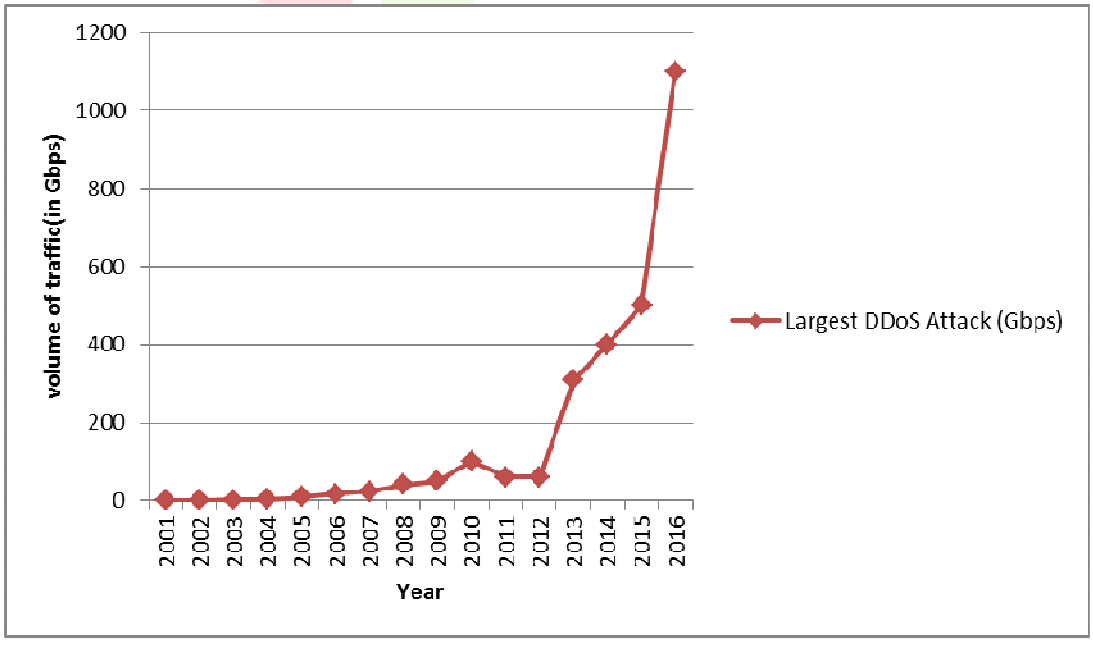

Figure 3.1: Year wise listing of DDoS attack volume in Gbps

There are various mechanism to mitigate from these attacks including redirecting from the DNS server which redirects the flooded DOS traffic packets from the targeted server to any other location and thus filtering the anomalous traffic. The redirection of anomalous traffic makes way for the normal traffic to move smoothly through the designated server and path. There are two widely used application and network layer mitigation techniques. In the first technique, the requests sent or received at the application layer are passed through different security services written in languages such as javascript, jsp etc. to parse the request to check the legitimacy of the used requests. It also employs cookies while parsing the requests. The later mitigation technique involves scrubbing and NULL routing. The null routing redirects the malicious traffic to a non-existent ip address. But this technique also involves the problem of false positive signals rate. The scrubbing technique segregates the packets by examining the header contents of the packets. This technique works well with the existing known attack patterns and does not work well with new attack patterns. The authors also summarized the DOS attacks traffic on the internet every year from year 2001 to 2016 in table 3.1. Figure 3.1 depicts the graphical representation of the data given in table 1. Before 2012 the frequency of attacks was increasing constantly. There is a steep increase in attack volume from year 2012 to 2016 **[19]**.

IV. CONCLUSION

This survey paper shows detailed study about various DoS and DDoS attacks that are smurf, UDP, TCP, SYN, Fraggle, ping. This paper also contains information about various defense techniques against these DoS and DDoS attacks. This paper also contains year wise set records in terms of the volume of traffic (in gigabits per second, or Gbps) from the year 2000-2016. DDoS attacks despite being in existence for a very long time are still one of the highest threats to security all over the internet. The ease of access to the attack tools is one of the main reasons behind DDoS being a security threat. The future work emphasis on practical implementation of DoS and DDoS detection algorithms using suitable machine learning techniques.

V. REFERENCES

[1] Bandara, K.R.W.V., Abeysinghe T.S., Hijaz A.J.M., Darshana D.G.T., Aneez H., Kaluarachchi S.J., Sulochana K.V.D.L. and Dhammearatchi D., 2016. Preventing DDoS attack using Data Mining Algorithms.

[2] Sahi A., Lai D., Li Y., Diykh M., 2017. An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment.

[3] Prasad M. K., Reddy M. R. A., Rao V. K., 2014. DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms – A Survey.

[4] Sachdeva M., Singh G., Kumar K., Singh K., 2009. Comprehensive Survey of Distributed Defense Techniques against DDoS Attacks.

[5] http://blogs.getcertifiedgetahead.com/dos-smurf-fraggle-attacks last accessed 17/02/18 18:45.

[6] https://en.m.wikipedia.org/wiki/WinNuke last accessed 17/02/18 19:04PM.

[7] https://www.incapsula.com/ddos/attack-glossary/ntp-amplification.html last accessed 17/02/18 19:25.

[8] https://www.incapsula.com/ddos/attack-glossary/syn-flood.html last accessed 17/02/18 19:45.

[9] https://www.tripwire.com/state-of-security/featured/5-notable-ddos-attacks-2017/ last accessed 18/02/18 15:45.

[10] Financial and reputational impacts of DDoS attacks: http://www.channelpronetwork.com/article/financial-and-reputational-impact-ddos-attacks, last accessed 25/02/18 10:20.

[11] Kaur P., Bijalwan A., Joshi R.C., Awasthi A. (2018) Network Forensic Process Model and Framework: An Alternative Scenario. In: Singh R., Choudhury S., Gehlot A. (eds) Intelligent Communication, Control and Devices. Advances in Intelligent Systems and Computing, vol 624. Springer, Singapore

[12] Awasthi, A., Hothi, N., Kaur, P., Singh, N., Chakraborty, and M., Bansal, S., 2017. Elucidative analysis and sequencing of two respiratory health monitoring methods to study the impact of varying atmospheric composition on human health. Atmospheric Environment 171: 32-37

[13] Agarwal, R., Awasthi, A., Mittal, S., Singh, N., and Gupta, P. K. 2010. Effects of air pollution on respiratory parameters during the wheat-residue burning in Patiala Journal of medical engineering & technology 34 (1), 23-28

[14] Distributed Denial-of-Service Attacks in the Internet Master's Thesis in Computer Science and Information Systems 20/12/2005.

[15] Zuckerman E., Roberts H., McGrady R., York J., Palfrey J., 2010. Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites.

[16] Lee Y. and Lee Y., 2011. Detecting DDoS Attacks with Hadoop.

[17] Priyadharshini1 V., Kuppusamy K., 2012. Prevention of DDOS Attacks using New Cracking Algorithm.

[18] DDoS Threat Landscape Report (2013-2014).

[19] https://qz.com/860630/ddos-attacks-have-gone-from-a-minor-nuisance-to-a-possible-new-form-of-global-warfare/ last accessed 25/02/18 11:00

[20] Lyon B., 2015. DDoS 2015: Understanding the Current and Pending DDoS Threat Landscape.

[21] Anwar R., Gorasia S., 2016. Detection and Classification of Distributed Denial of Service (DDoS) Attack.

[22] Somani G., Gaur M.S., Sanghi D., Conti M., Rajarajan M.K. Buyya R., 2017. Combating DDoS Attacks in the Cloud: Requirements, Trends, and Future Directions.