Comprehensive Survey on DDOS attack with its mitigation Techniques

Harmeet Kaur Dhaliwal
Research Scholar
Department of Computer Science and Engineering,
Chandigarh Engineering College,
Landran, Mohali, India
dhaliwal.harmeet@yahoo.com

Jashanpreet Singh
Assistant Professor
Department of Computer Science and Engineering,
Chandigarh Engineering College,
Landran, Mohali, India
cecm.cse.jashan@gmail.com

Abstract— The remarkable development and accomplishment of Internet has changed the way customary vital administrations, for example, managing an account, transportation, prescription, training and guard are worked. Presently they are as a rule logically supplanted by less expensive and more effective Internet-based applications. In present time, the world is exceedingly reliant on the Internet and it is considered as principle foundation of the worldwide data society. Hence, the accessibility of Internet is extremely basic for the financial development of the general public. In any case, the natural vulnerabilities of the Internet engineering give chances to a considerable measure of assaults on its base and administrations. Appropriated foreswearing of-administration assault is one such sort of assault, which represents a colossal danger to the accessibility of the Internet. One of the greatest difficulties before scientists is to discover subtle elements of these assaults in light of the fact that to stay away from slander the majority of the business locales don't uncover that they were assaulted. In this paper, an outline of DDOS issue and Inherent vulnerabilities in the Internet engineering are given.

Index terms— DDOS Attack, Security, Internet, Business.

1. INTRODUCTION

DDOS simply stands for “Distributed Denial of service” as in simple manner denying the service as provided by some kind of device or any resource. In networking this term usually situates with bandwidth as we all are familiar with internet that connects us all. So, here the DDOS attack can be simply depicted by unable to access a webpage. This defines the DDOS as the type of attack in which the bandwidth from a particular resource to a host is cut-off. The reason can be many like hacking, traffic excess and many more but mostly the attackers use this as their weapon to hamper proper functioning of the resource. For e.g.-a website of a bank is made unavailable for sometimes, it may sound nothing is wrong but the technical community knows something big is wrong. This is how attackers loot cash online from bank websites.

In an example, DDOS attack can be simply compared to any server that is handling client requests. The server can simply be in denial of service if numbers of requests are passed onto it at a time, it may cause it to crash or it may become un-responsive, same is the case with web servers that are under DDOS attacks which either crashes or become unresponsive. Meanwhile here comes the concept of the IP address as we know in a network there are addresses provided to the users, the DDOS attackers held up the criteria of IP address spoofing I.e. forging. The utmost motives for these attacks may vary depending upon the type of attackers but mostly these can occur due to cash, revenge or sabotage etc. Their main weapon is distributed networks where it is not much easy to get hold of things that from where the network is being attacked that gives the attackers the free flow to act upon the network for a certain period of time. To answer these flaws for not being able to identify the attacks for certain networks DDOS II was proposed that launches a defense mechanism within the network thereby blocking the network segment from where the attack is originating. it also answers the distributed systems by fully blocking it from the internet without allowing system crash that carries much importance.

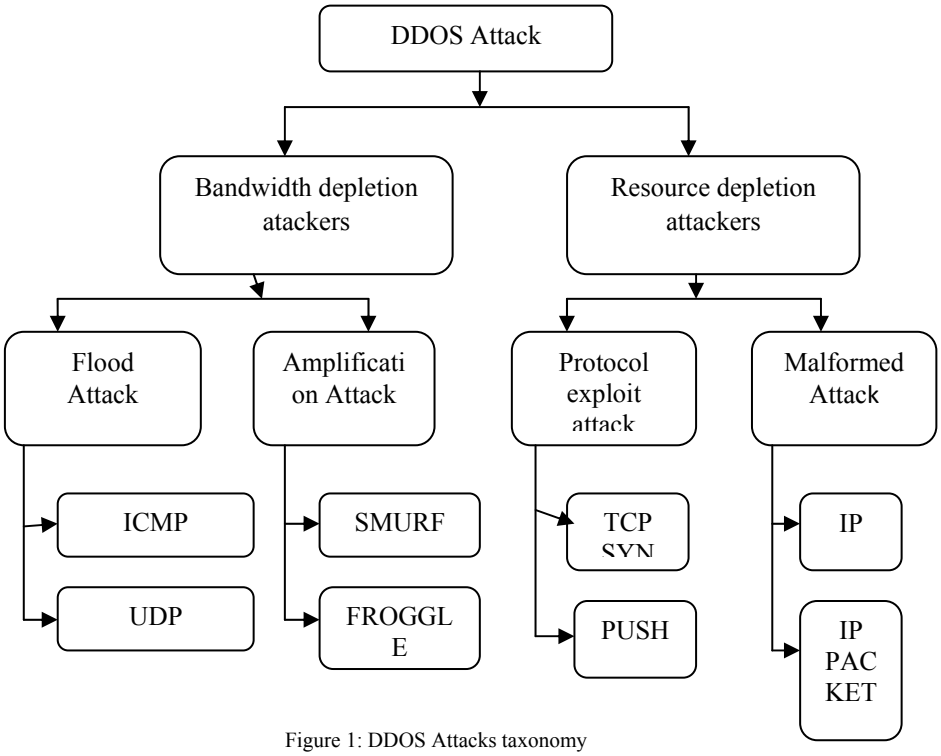

Figure 1: DDOS Attacks taxonomy

DDOS attacks have become much more common that they are practiced by many anonymous groups either for their own benefit or just for revenge. The question arises now-Is there any way to prevent these attacks. The answer to the question remains simple as there is no efficient way to stop these attacks but there are some guidelines to reduce their likelihood of attacker attacking the network. These can be listed as:

A. Anti-virus

The most commonly used term these days but not all of us pay much attention to it. Most of the attacks enter our network in the form known to be viruses which can get easily ignored if a proper good quality anti-virus is not monitoring things. So, anti-virus remains first thing for preventing these attacks.

B. Firewall

In simple terms it is a wall that filters what can enter the network and what cannot. The network with no firewall becomes much more vulnerable to these attacks. So proper firewalls need to be maintained to keep an eye out on what is entering and leaving the network.

C. E-mail spam

If asked to a common person that your email address possess more than you think, the individual simply ignores thinking it just as an email address. When we respond to certain spam emails, they can simply harvest information regarding the organization and everyone knows how much destructive it is for organizations whose information is possessed by an outsider. So this emphasis on handling Spams more carefully.

The Poor State of Cyber Security has at long last started to pull in wide consideration what's more, worry outside the group of PC security specialists. This is a welcome improvement since, regardless of whether the most exceedingly bad fears of a "computerized Pearl Harbor" are practical, plainly digital assaults force overwhelming expenses and that the rate of assault is increasing. Security vulnerabilities keep on being found and unveiled in generally conveyed programming at an extraordinary rate. However, web associated PC clients by and large neglect to find a way to fix the vulnerabilities in their product and to defend their frameworks from vindictive code. Regardless of the huge amassed misfortunes and notices of more genuine threats, the web remains a position of digital shakiness.

Digital security is not a solitary issue, yet rather a gathering of altogether different issues including different arrangements of dangers, targets and expenses. Therefore, legitimate approach investigation must start by distinguishing the specific issue to be considered.

This paper concentrates on a type of digital assault known as an appropriated refusal of administration assault ("DDOS"). DDOS assaults are fascinating from the lawful point of view since there is basically nothing that a casualty can do to ensure itself, also, on the grounds that the genuine culprits of the assaults are about difficult to

follow at present. Therefore, if the law wishes to demoralize DDOS assaults, some other object of lawful weight must be picked.

One underlying driver of DDOS assaults is uncertain programming. Insecurities in programming programs that have been broadly conveyed on web associated PCs are misused with a specific end goal to recruit PCs into a multitude of "zombies" that is later utilized by an aggressor to dispatch the DDOS assault. An appropriately working programming business sector may be relied upon to create the best possible equalization of cost and quality attributes (counting the level of security). In any case, for reasons that will be talked about in more prominent detail later, for example, the presence of "frailty externalities," it is conceivable that interest in security is instantly lacking.

Some of the used techniques to somewhat limit DDOS attacks:

- Making policies and procedures
- Keeping product updated design n testing
- Patch management
- Auditing
- By implementing uRPF.
- Cisco implementation methodology
- Jupiter implementation methodology
- Management and control plane protection
- Using one Any of FW/IDS/IPS
- Using router engine protection
- Prefix filtering

2. RELATED WORK

Abley Joe [16] "ISC Technical Note Series, Hierarchical Any cast for Global Service Distribution" proposed an intrusion based system that uses particular Irc ports to communicate between clients and agents also known Irc based agent handler. It allows communications through separate channels thus hampering DDOS attacks.

The BGP TTL Security Hack [17] was proposed by Gill, Vijay, John Heasley, and David Meyer to handle the CPU overloading attacks, so it proposed a mechanism that is based on expected TTL values which can help provide simple and reasonably robust defenses from the infrastructure attacks based on forged BGP packets.

A document [18] was proposed under "Dissemination of flow specification rules, draft marques idr flow spec 00.txt" the engineering task force to encode rules as a BGP NLRI which can be reused for several different control applications. The required mechanisms to utilize this definition to the problem of immediate concern to the authors: intra and inter provider distribution of traffic filtering rules to filter (Distributed) Denial of Service (DOS) attacks. The choice of BGP was justified by the fact that the key issues in terms of complexity are problems which are common to unicast route distribution and have already been solved in the current environment.

At Cisco [19] IOS Security Configuration Guide, Unicast RPF feature helps one mitigate problems that are caused due to forged (spoofed) IP source addresses into a network by discarding IP packets which lack a verifiable IP source address.

3. COMPARISON OF TECHNIQUES

Author	Year	Technique	Advantages
Abley and Joe	2000	Intrusion Based System	Allows communications through separate channels
Gill et al	2003	BTSH	On expected TTL values which can help provide simple and reasonably robust defenses from the infrastructure attacks based on forged BGP packets
Marque et al	2003	BGP	Intra and inter provider distribution of traffic filtering rules to filter (Distributed) Denial of Service (DOS) attacks.
Cisco IOS Security Configuration Guide	2003	Unicast RPF feature	Discarding IP packets not having valid source address.

4. CASE STUDIES OF DDOS ATTACK VULNERABILITIES

A. CASE STUDY 1: ANONYMOUS TARGET BANK OF GREECE WEBSITE WITH MASSIVE DDOS ATTACK

The online hacktivist Anonymous as of late relaunched operation OpIcarus coordinated towards saving money part in Europe and the United States — The primary bank going under the flame is the Bank of Greece who had their site under a progression of conveyed denial of-service assaults (DDoS) compelling the servers to remain disconnected for over 6 hours. OpIcarus is about focusing on keeping money and budgetary mammoths Anonymous' Operation OpIcarus was dispatched in January 2016 and restarted in March 2016. The hacktivists behind the operation trust banks and budgetary mammoths are included in debasement and to enroll their challenge they needed to take the war to a next level. In a select discussion with one of the hacktivists behind the Greek bank DDoS assault, HackRead was informed that: "The greek national bank has been disconnected throughout the day. We might want all banks out there to realize that unless they consider themselves responsible for their wrongdoings against humankind that we will strike another bank each and every day and rebuff them #OpIcarus."

B. CASE STUDY 2: KKK WEBSITE SHUT DOWN BY ANONYMOUS GHOST SQUAD'S DDOS ATTACK

The Anonymous versus Ku Klux Klan (KKK) digital war is understood to every one of us. In continuation of that war, Anonymous offshoot Ghost Squad cut down one of real site having a place with the KKK individuals. In a progression of effective conveyed foreswearing of-administration (DDoS) assaults only a couple of hours back, Anonymous has closed down the official site of Loyal White Knights of the Ku Klux Klan (KKK). Phantom Squad, the gathering said to be behind this assault works with the online hacktivist Anonymous. The purpose behind assaulting the KKK is the "obtuse prejudice" for the sake of free discourse. In a select discussion with one of the assailants, HackRead was informed that: "We focused on the KKK because of our programmers being up in their face, we have confidence in free discourse yet their type of convictions is solid and shrewdness. We remain for protected rights however they need any individual who is not Caucasian expelled from earth so we focused on the KKK official site to show love for our boots on the ground and to communicate something specific that all types of debasement will be battled. We are not rightist but rather we surely don't concur with the KKK development. They are the Fascists and they are the Racists." A mistake message "The kkkknights.com page isn't working" is shown for those meeting the site. KKK has not interestingly go under assaults by Anonymous. Prior, the hacktivists unveiled individual data of KKK individuals. In October 2015, the gathering additionally did DDoS assaults on KKK's site, as one of the Klan individuals clearly bugged a lady on Twitter.

5. DDOS ATTACK DEFENCES

The primary point of a DDoS protection framework is to mitigate casualty's assets from high volume of fake parcels sent by assailants from circulated areas, so that these assets could be utilized to serve authentic clients. Underneath different procedures for the relief of DDOS assault has been displayed.

Xiao et al. [8] present a methodology that utilizations data hypothesis and GA to distinguish unusual system practices. Taking into account the common data between system highlights and the sorts of system interruptions, a little number of system components are firmly related to network assaults. At that point a direct structure principle is determined utilizing the chose highlights and a GA. The utilization of common data lessens the multifaceted nature of GA, and the single coming about direct run makes interruption recognition productive continuously environment. Be that as it may, the methodology considers just discrete elements. Li [9] present to identify system peculiar utilizing Genetic Algorithm. The recognition rates might be expanded because of quantitative elements consideration. Parameters and development forms for GA are talked about in subtle elements and executed. This methodology utilizes advancement hypothesis to data development with a specific end goal to channel the activity information and along these lines diminish the many-sided quality. To execute and measure the execution of this framework they utilized the KDD99 benchmark dataset and got sensible recognition rate. Spans [10] executed a technique to recognize both inconsistencies and system abuses by brushing Genetic Algorithm‟s and Fuzzy information mining advances. In this technique select the most huge system includes and find the most ideal parameters of the fluffy capacity by utilizing Genetic Algorithm. Crosbie [11] proposed a system to identify system oddities utilizing Genetic Programming (GP) and numerous operator innovation. At the point when the specialists are not legitimately introduced, the preparation procedure takes long time. The correspondence among little self-governing operators is still an issue. Selvakani [12] Applied Genetic Algorithm to produce rules for preparing the IDS. Guidelines are produced for just Smurf (DoS) assault and Warzemaster (R2L) assault. This execution of this procedure recognition rate is low. This review demonstrates that the proposed Intrusion Detection models for R2L, U2R, Probe assaults get low identification rates utilizing KDDCup dataset. This paper considers two sorts of assaults for every classification i.e., DoS, R2L, U2R and Probe. Watched every one of the elements in the KDDCUP Dataset to identify the assaults. Lu [13] Develop a technique to infer an arrangement of characterization standards by utilizing Genetic Programming (GP) with help of past information of system. In this strategy utilizing GP the viable execution is

more troublesome because of the framework required more information or time. In [14] the creators exhibited a vigorous neural system indicator for Distributed Denialof-Service (DDoS) assaults in PCs giving Internet administrations. A hereditary calculation was utilized to choose a little number of proficient components from an expanded arrangement of 44 measurable elements, which are assessed just from the bundle headers. Most regulated neural net models require retraining to enhance examination capacity because of changes in the info information, yet unsupervised net offers expanded level of flexibility to neural nets and can progressively enhance their investigation ability. The vast majority of the system based frameworks in unsupervised based IDSs utilized self-sorting out maps (SOMs) neural nets and just a couple of frameworks utilized different sorts of unsupervised neural nets. In [15], various SOMs are utilized for interruption discovery, where a gathering of more particular maps is utilized to process system activity for every convention independently. Each neural net was prepared to perceive the ordinary action of a solitary convention. It for the most part breaks down the capability of the Kohonen self-sorting out guide to contract the envelope of meddling practices that would not be gotten by an identification framework.

6. PARAMETERS FOR EVALUATION

A. Packet Delivery Ratio

It is defined as the total no. of packets sent divided by the total no. of packets in the network;

$$\mathrm{PDR} = \frac{1}{\mathrm{np}} \sum_{u=1}^{\mathrm{np}} \frac{\mathrm{pcktd_u}}{\mathrm{pcks_u}} \qquad (1)$$

B. End-to-End Delay

It is defined as the delay in the total no. of packets sent divided by the total no. of packets in the network;

$$\mathrm{E} = \frac{1}{\mathrm{np}} \sum_{u=1}^{\mathrm{np}} \frac{\mathrm{dn_u}}{\mathrm{pckdn_u}} \qquad (2)$$

C. Throughput

This is defined as the total packets sent in the network divided by the total no. of data packets;

$$\mathrm{T} = \frac{1}{\mathrm{np}} \sum_{u=1}^{\mathrm{np}} \frac{\mathrm{td_u}}{\mathrm{t_u}} \qquad (3)$$

7. CONCLUSION AND FUTURE SCOPE

While the range of attacks that can be performed on targets is as broad as the spectrum of constructive technology itself, this thesis deals with a particular class of attacks known as Distributed Denial of Service (DDoS) attacks. Distributed Denial of Service (DDoS) attacks are a scaled form of DoS attacks where multiple attack bots2 are employed in a coordinated fashion to form an attack network for attacking a specific target. DDoS attacks are catastrophic particularly when applied to highly sensitive targets like Critical Information Infrastructure.So, prevention of DDOS attacks are very necessary.

ACKNOWLEDGMENT

I wish to express my sincere gratitude to Mr. Jashanpreet Singh, Assistant Professor for his guidance and encouragement in my review. I would also like to thank my fellow mates Manpreet Singh and Hardavinder Singh for their suggestions throughout the work.

REFERENCES

[1] Ravi Sharma, “Study of Latest Emerging Trends on Cyber Security and its challenges to Society”, International Journal of Scientific & Engineering Research, Vol. 3, 2012

[2] Abraham D. Sofaer, David Clark, Whitfield Diffie , “Proceedings of a Workshop on Deterring Cyber Attacks”, Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.htmlCyber Security and International Agreements ,Internet Corporation for Assigned Names and Numbers, pp. 185-205, 1997.

[3] I.Ogechi, I.Chukwugoziem, H.C.Inyiama. "Fuzzy modelling of a network Denial of Service (DoS) attack phenomenon," International Journal of Engineering & Technology, Vol. 5, No. 2, 2013

[4] L.Feinstein, D.Schnackenberg, R. Balupari,D. Kindred, "Statistical approaches to DDoS attack detection and response," In DARPA Information Survivability Conference and Exposition, Washington DC, Vol. 1, pp. 303-314, 2003.

[5] J. Choi, C. Choi, Byeongkyu Ko, D. Choi, P. Kim. "Detecting Web based DDoS Attack using MapReduce operations in Cloud Computing Environment," Journal of Internet Services and Information Security, Vol. 3, no. 3/4, pp. 28-37, 2013.

[6] Loren Paul Rees, Jason K. Deane , Terry R. Rakes , Wade H. Baker, “Decision support for Cyber security risk planning”, Department of Business Information Technology, Pamplin College of Business, Virginia Tech., Blacksburg, VA 24061, United States b Verizon Business Security Solutions, Ashburn, VA 20147, United States.

[7] Carr, V and J.H.M. Tah, “A fuzzy approach to construction Project management system”, J. Adv. Eng. Software, Vol.32, pp. 847-857, 2001.

[8] T. Xiao, G. Qu, S. Hariri, and M. Yousif, “An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm”, Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC „05), Phoenix, AZ, USA. 2005. Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Net, 2005.

[9] W. Li, “Using Genetic Algorithm for Network Intrusion Detection”. “A Genetic Algorithm Approach to Network Intrusion Detection”. SANS Institute, USA, 2004.

[10] Bridges, Susan, Rayford B. Vaughn,“ Intrusion Detection via Fuzzy Data Mining”, In Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp. 109-122, Ottawa, Canada, 2000.

[11] Crosbie, Mark, Gene Spafford,"Applying Genetic Programming to Intrusion Detection", In Proceeding of 1995 AAAI Fall Symposium on Genetic Programming, pp. 1-8, Cambridge, Massachusetts, 1995.
[12] Selvakani S, R.S. Rajesh," Genetic Algorithm for framing rules for Intrusion Detection", IJCSNS, Vol.7, No.11, 2007.
[13] W. Lu, I. Traore,"Detecting new forms of network intrusion using genetic programming", Computational Intelligence Vol.20, Issue 3, pp. 475-494, 2004.
[14] J. Cannady, "Artificial Neural Networks for Misuse Detection", In Proceedings of National Information Systems Security Conference, 1998.
[15] B.C. Rhodes, J.A. Mahaffey, and J. D. Cannady, "Multiple Self-Organizing Maps for Intrusion Detection", In Proceedings of 23rd National Information Systems Security Conference, 2000.
[16] Abley, Joe — "ISC Technical Note Series, Hierarchical Anycast for Global Service Distribution." 2003. Internet Software Consortium, 17 Aug. 2003.Ļ.
[17] Gill, Vijay, John Heasley, and David Meyer — "The BGP TTL Security Hack (BTSH)." May 2003. 18 Aug. 2003.
[18] Marques, Pedro, NischalSheth, Robert Raszuk, Jared Mauch, and Danny McPherson — "Dissemination of flow specification rules, draft-marques-idr-flowspec-00.txt." June 2003. The Internet Engineering Task Force, Internet-Drafts. 14 Jul. 2003. . Weaver — "How to 0wn the Internet in Your Spare Time." Proceedings of the 11th Usenet Security Symposium, San Francisco, CA. 5- 9 Aug. 2002. USENIX Association. 14 July 2003.
[19] "Configuring Unicast Reverse Path Forwarding." Cisco IOS Security Configuration Guide, Release 12.2. 17 Aug. 2003. 2003.<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.pdf>.

AUTHORS PROFILE

Harmeet kaur Dhaliwal, presently a research scholar and pursuing M.tech at Chandigarh Engineering College in the department of Computer Science and Engineering. She has completed her graduation in 2012. Her research work includes the prevention of Denial of Distributed Service Attacks (DDoS) using fuzzy logic. The implementation was done using MATLAB tool. She has also carried out projects on Java.

Jashanpreet Singh, an Assistant Professor at Chandigarh Engineering College, Mohali. He also completed his masters from Chandigarh Engineering College in 2014. He has done his graduation from Lovely Professional University in 2011. His domain area is Android development and carried out many projects in the same.