International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.3., 2016
(May-June)

REVIEW ARTICLE

ISSN: 2321-7758

# DENIAL OF SERVICE ATTACK AND ITS PREVENTION TECHNIQUES

**ALPNA[1], Dr SONA MALHOTRA[2]**
[1]Mtech Student, [2]Assistant Professor
University institute of engineering and technology
Kurukshetra University, Haryana, India

**ABSTRACT**

In today's world, Internet is the primary medium for communication among the number of users across the network. Due to this vulnerability to enhance cyber crimes increases and there has been an enormous increase in the number of DOS (denial of service), DDOS (distributed denial of service attack) attacks on the internet over the past decade. Amongst various online attacks hampering IT security, Denial of Service (DoS) has the most devastating effects. Network resources such as network bandwidth, web servers and network switches are mostly the victims of DDoS attacks. Distributed Denial of Service attack is a coordinated attack, generally performed on a massive scale on the availability of services of a target system or network resources. Due to the continuous evolution of new attacks and ever-increasing number of vulnerable hosts on the Internet, many DDoS attack detection or prevention mechanisms have been proposed. In this paper, we present a comprehensive study of DOS, DDoS attacks, their types, detection methods and tools used in networks. The paper also highlights open issues, research challenges and possible solutions in this area.

Keywords: DOS, DDOS, types of DOS attack, prevention methods, mitigation techniques.

## I.INTRODUCTION

Denial-of-service (DoS) attack is an attempt which makes a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Denial of service attacks are designed to consume resources so that other users are unable to use the resources and are therefore "denied service". In a computer network environment, the key resources are CPU, memory, and bandwidth.

- By consuming CPU resources a DoS attack can prevent a network device from responding to management requests or processing packets, effectively locking up the device.
- By consuming memory resources a DoS attack can prevent a network device from processing packets, effectively locking up the device.
- By consuming bandwidth resources a DoS attack can reduce the speed and volume of legitimate network traffic.

Symptoms of Dos attack to include:

- Performance of network is slow.
- Unavailability of a particular website.
- We are not to access any website.
- The no of spam email increases

Nowadays, DoS attacks are usually launched in a distributed way the attack traffic is from many attacking sources and the aggregated traffic volume is so big that it can easily deplete the victim's key computing resources, such as bandwidth and CPU time. The combination of multiple machines to launch a Denial-of-Service attack, this becomes a Distributed Denial of Service (DDoS) attack. DDoS means when the source of the attack is not coming from a single source, but multiple source. DDoS cannot be eliminated with merely filtering the source IPs since it is often launched from multiple points installed with agents. Some known DDoS tools are Mstream, Trinoo, TFN2K (Tribe Flood Network), Stacheldraht and Shaft. DDoS attack is an example of a bandwidth attack.

In the distributed form of DoS attacks (called DDoS), The attackers typically target site or service hosted on high-profile web servers such as bank, credit card payment gateways, mobile phone networks and even root name servers. Buffer overflow technique is employed to commit such kind of criminal attack known as spoofing the attacker first takes control of a large number of vulnerable hosts on the internet, and then uses them to simultaneously send a huge flood of packets to the victim, exhausting all of its resources. There are a large number of exploitable machines on the internet, which have weak security measures, for attackers to launch DDoS attacks, so that such attacks can be executed by an attacker with limited resources against the large, sophisticated sites. The attackers in DDoS attacks always modify the source addresses in the attack packets to hide their identity, and making it difficult to distinguish such packets from those sent by legitimate users. DDoS attacks in the recent past, including the attacks on e-commerce sites like Yahoo, Amazon, Microsoft, and eBay.

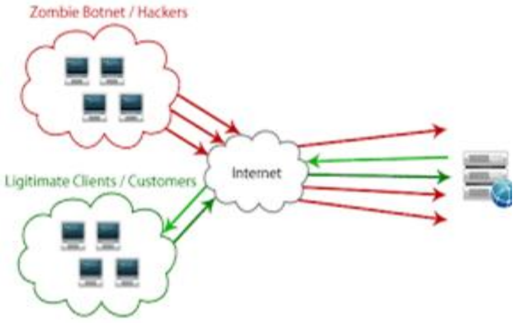

Fig 1.DDos attack [18]

## II. TYPE OF ATTACKS

There are several flavors of Denial of Service that could disrupt a normal service.

- One is bandwidth depletion. This method is to congest the network, massive use of the bandwidth then lead the network breakdown.
- The other type is resource depletion. Attacker depletes the key resources such as CPU, memory and so on. Then break the server. The attack usually starts from numerous sources to aim at a single target. Multiple target attacks are less common; however, there is the possibility for attackers to launch such type of attack Spoofed, altered, or replayed routing information

**1. Flood attack**: this is the earliest form of dos attack and also known as ping flood. It is based on an attacker simply sending the victim overwhelming number of ping packets, usually by using the” ping” command, which result into more traffic than the victim. It is very simple to launch, but to prevent it completely is the most difficult.

**2. Ping of death attack:** the ping of death attack sends oversized internet control message protocol (ICMP) packets, and it is one of the core protocols of the IP suite. It is mainly used by networked computer’s OS to send error message indicating datagram to the victim .the maximum packet size allowed is 65536 octets. Some systems, upon receiving the oversized packets, will crash, freeze pr reboot, resulting in Dos.

**3. SYN attack:** it is also termed as TCP SYN flooding. In the transmission control protocol (TCP), handshaking of network is done with SYN and ACK message. An attacker initiates the TCP connection to the server with an SYN. The server replies with an SYN-ACK. The client then does not send back an ACK causing the server to allocate memory for the pending connection and wait. This fills up the buffer space for SYN messages on target system, preventing other system on the network from communicating with the target system.

**4. Teardrop attack:** The teardrop attack is an attack where fragmented packets are forged to overlap each other when the receiving host tries to resemble them. IP's packet fragmentation algorithm is used to send corrupted packets to confuse the victim and may hang the system. This attack can crash the various Oss due to a bug in their TCP/IP fragmentation reassembly code.

**5. Smurf attack:** it is a way of generating significant computer network traffic on a victim network. This is a type of DOS attack that floods a target system via spoofed broadcast ping message. This attack consists of a host sending an ICMP echo request to a network broad cast address. Every host on network receives the ICMP echo request and sends back an ICMP echo response inundating the initiator with network traffic. On a multi-access broadcast network, hundreds of machines might reply to each packet. In a smurf attack, the attacker sends ICMP echo request (ping) packets to an intermediary device.

**6. TCP Reset Attack:** TCP reset also utilize the characteristics of TCP protocol. By listening the TCP connections to the victim, the attacker sends a fake TCP RESET packet to the victim. Then it causes the victim to inadvertently terminate its TCP connection.[1]

**7. UDP storm attack:** This kind of attack can not only impair the hosts. Services, but also congest or slow down the prevailing network. When a connection is established between two UDP services, each of which produces a very huge number of packets, thus cause an attack. [1]

**8. DNS request attack:** In this attack scenario, the attack sends a large number of UDP-based DNS requests to a name server using a spoofed source IP address. Then the name server, acting as an intermediate party in the attack, responds by sending back to the spoofed IP address as the victim destination. Because of the amplification effect of DNS response, it can cause serious bandwidth attack. [6]

**9. CGI request attack:** By simply sending multiple CGI request to the target server, the attacker consumes the CPU resource of the victim. Then the server is forced to terminate its services. [1]

**10. Mail bomb attack:** A mail bomb is the sending of a enormous amount of e-mail to a specific person or system. A huge amount of mail may simply fill up the recipient's disk space on the server or, in some cases, may be too much for a server to handle and may cause the server to stop working. This attack is also a kind of flood attack. [7]

**11. Algorithmic complexity attack:** It's a class of low-bandwidth DDoS attacks that exploit algorithmic deficiencies in the worst case performance of algorithms used in many mainstream applications. For example, both binary trees and hash tables with carefully chosen input can be the attack targets to consume system resources greatly. [7]

**12. Spam Attack:** This type of attack is used for targeting the various mail services of corporate as well as public users. DDoS attack through spam has increased and disturbed the mail services of various organizations. Spam penetrates through all the filters to create DDoS attacks, which causes serious trouble to users and the data. But these smail services are frequent target of hackers and spammers. [1]

## III.HOW TO PROTECT FROM DOS/DDOS ATTACK

1). Implement router filters. This will lessen your exposure to certain DoS attacks. Firewalls can effectively prevent users from launching simple flooding type attacks from machines behind the firewall. Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. [3]

2). If such filters are available for your system, install patches to guard against TCP SYN flooding. Today, many DDoS attacks exploit vulnerabilities in target system. So removing known security holes by installing all relevant latest security patches prevents re-exploitation of vulnerabilities in the target system

3). Disable any unused or inessential network service to avoid attack. The less there are applications and open ports in hosts, the less there are chance to exploit vulnerabilities by attackers. Therefore, if network services are not needed or unused, the services should be disabled to prevent attacks, e.g. UDP echo, character generation services. [3]

4). Enable quota system on your OS if they are available. You can often configure both your operating system and your applications to be more resilient to application layer DDoS attacks. Things such as ensuring enough inodes on your Linux server to configuring the right number of Apache worker threads can help make it harder for an attacker to take down your service

5). Install latest security patches: Today, many DDoS attacks exploit vulnerabilities in target system. So removing known security holes by installing all relevant latest security patches prevents re-exploitation of vulnerabilities in the target system. [3]

6). Establish and maintain regular backup schedules and policies, particularly for important configuration information about network.

7). Establish and maintain appropriate password policies, especially access to highly privileged accounts such as UNIX root or Microsoft Windows NT administrator.

8). Automated Mitigation - Many tools will monitor netflow data from routers and other data sources to determine a baseline for traffic. If traffic patterns step out of these zones, DDoS mitigation tools can attract the traffic to them using BGP or other mechanisms and filter out noise. They then pass the clean traffic further into the network. These tools can generally detect both volumetric attacks, and more insidious attacks such as slowloris.

## IV. MITIGATIONS TECHNIQUES FOR DDOS ATTACK

1. SOS [9] is the first solution that uses an overlay network to mitigate DDoS attacks. The basic idea is using the overlay network to hide the real location of the protected server. A packet from a legitimate client is forwarded through the overlay network in a anonymous manner and finally reaches a special overlay node (servlet), whose identity is hidden. Only the servlet can forward the packet to pass through the perimeter routers of the server.

2. MOVE [10] and Multipath-Overlay [11] provide mechanisms for the overlay nodes to filter out illegitimate packets. MOVE uses SSL and Multipath-Overlay uses UMAC plus AES. For protecting the connection setup phase, MOVE and Multipath-Overlay push the task of distinguishing spurious requests to overlay nodes who may accept all the connection requests, due to the lack of the local knowledge of the server. These two solutions also suggest using Graphic Turing Test (GTT) for filtering out requests from remotely controlled zombie machines. However, GTT needs humans involved and is not transparent to users.

3. OverDose [12] protects the connection setup phase by using crypto-puzzles. Each request packet should contain a correct solution of a puzzle generated with the current puzzle seed (which is changed periodically), and packets with correct solutions of puzzles in higher levels have priority for being forwarded. Since the total computational power of the adversary is bounded, there exists a puzzle level such that the adversary cannot generate enough packets with correct solutions for the puzzles in that level to flood the connection setup channel. However, in OverDose there is no mechanism to prevent a host from reusing solutions of the same puzzle.

4. SIEVE [13] has lighter design complexity and achieves competitive performance to it. First, a puzzle based solution needs a seed generator, which usually is the protected server. In SIEVE, there is no need for the server to get involved in the protection of connection setup phase. Second, in SIEVE the clients do not need to do any extra computation except for sending back the requests with cookies; while in the puzzle-based solution the clients need to find solutions for the puzzles. Third, if the compromised hosts have equal computational power as the legitimate hosts, then the puzzle-based solution achieves per-host fairness which is similar to SIEVE. However, the adversary can always flood spurious.

5). CluB [14] can collaborate with different routing. Policies in the network, including contemporary datagram options. They estimate the effectiveness of the method and also study a set of factors for tuning the granularity of control.

6). STONE a stream-based DDoS defense framework, and describe a methodology to pipeline traffic profiling and detection of DDoSattacks, as well to enable mitigation and filtering, by monitoring a limited set of traffic characteristics. They also describe how the methods can be efficiently implemented using a streaming engine (StreamCloud) that enables parallelization. The efficiency and effectiveness of the methods are studied involving volumes of network traffic that include data from available attack data traces, injected in traffic samples of a large backbone link.

7.) An efficient method to detecting and mitigation against TCP SYN flooding attacks using Three Counters Algorithm, which detects spoofed IP packets up to 80%.

In SYN floods, attacker would send a quick barrage of SYN packets from IP addresses (often spoofed) that will not generate replies to the SYN/ACKs. To remain effective, attacker needs to send new barrages of bogus connection requests frequently. Most of the SYN flooding packets would not be retransmitted. On the other hand, if a SYN packet is lost, it would retransmit the SYN packet several times before giving up. The mitigation scheme utilizes the characteristic of SYN floods and client's persistence. They use three counting filters to record related information:

- C-1: to record the first SYN packets of each connection;
- C-2: to record the SYN packets, whose connections have completed the three-way handshake?
- C-3: to record the other SYN packets. [15]

8. CAPTCHA develops a working prototype that detects and mitigates HTTP based DDoS attacks; there must be adequate design of a system before it can be implemented. The system was designed so that it could be deployed in a Distributed environment. The system also integrates directly with Apache making deployment of the Detection module (Mitigate.c) exceptionally easy for any novice IT administrator to set up. The problem scenario is when too many hosts (or compromised computers) request the website at the same time. The server cannot cope with the requests and service availability is affected. The system detects when an individual host has requested a website too many times and then requires that host to verify they are a human. Certain exceptions to this rule exist (for example, Search Engines are exempt from having to verify at all and are always given access to the site without hindrance). [16]

9.) Optimized HCF Filtering and window matrix techniques are to detect Distributed Denial of Service attack. The algorithm says that the packets are legitimate IP packets and spoofed IP packets along with their IP addresses. Based on this result, they conclude to accept or discard the packets.[17]

## CONCLUSION

We have studied various types of Dos and DDos attacks and what are the reasons behind the attack. To avoid the attack we have the different prevention techniques. The attacker uses the various types of tools to conduct the attack, so we have follow the preventions methods to avoid the loss.

## REFERENCES

[1]. Akash Mittal, Prof. Ajit Kumar Shrivastava, Dr. Manish Manoria, A Review of DDOS Attack and its Countermeasures in TCP Based Networks, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011.

[2]. Yao Chen1, Shantanu Das1, Pulak Dhar2, Abdulmotaleb El Saddik1, and Amiya Nayak, Detecting and Preventing IP-spoofed Distributed DoS Attacks, International Journal of Network Security, Vol.7, No.1, PP.70–81, July 2008.

[3]. B. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE, Distributed Denial of Service Prevention Techniques, urnal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010 1793-8163.

[4]. Aabdallah elhigazi abdallah,2 Shukor abd razak,3 Coulibaly yahaya, detection and prevention of denial of serviceattacks (dos) in wlans infrastructure, journal of theoretical and applied information technology 31st january 2015. vol.71 no.3, ISSN: 1992-8645.

[5]. A.Prathap , R.Sailaja, Detection and Prevention of Denial of Service Attacks Using Distributed Denial-of-Service Detection Mechanism, A.Prathap et al, /

(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (6), 2012,5434-5438,ISSN0975-9646.

[6]. A. Yaar, A. Perrig, and D. Song, "PI: A path identification mechanism to defend against DDoSattacks," in proceedings of the IEEE symposium on Security and Privacy, pp. 93-109, May 2003.

[7]. Elinor Mills, "Radio Free Europe DDOS attack latest by hactivists," Online at

[8]. http://news.cnet.com/8301-10784_3-9933746-7.html, CNET News, May. 2008.

[9]. A. D. Keromytis, V. Misra, and D. Rubenstein. Sos: secure overlay services. SIGCOMM Comput. Commun. Rev., 32(4):61–72, 2002.

[10]. A. Stavrou, A. D. Keromytis, J. Nieh, V. Misra, and D. Rubenstein. Move: An end-to-end solution to network denial of service. In In Proceedings of the ISOC Symposium on Network and Distributed System Security (SNDSS), pages 81–96, 2005.

[11]. A. Stavrou and A. D. Keromytis. Countering dos attacks with stateless multipath overlays. In Proceedings of ACM CCS, pages 249–259, New York, NY, USA, 2005. ACM.

[12]. E. Shi, I. Stoica, D. Andersen, and A. Perrig. Overdose: A generic ddos protectionservice using an overlay network. Technical report, Carnegie Mellon University,CMU-CS-06-114, 2006.

[13]. Zhang Fu, Marina Papatriantafilou, Philippas Tsigas, Mitigating Distributed Denial of Service Attacks inMultiparty Applications in the Presence of ClockDrifts, IEEE Transactions on Dependable and Secure Computing Volume 9.

[14]. Zhang Fu, Marina Papatriantafilou, Philippas Tsigas, CluB: A Cluster Based Framework for MitigatingDistributed Denial of Service Attacks ,Symposium on Applied Computing (SAC) TaiChung, Taiwan 21-24 March, 2011

[15]. S.Gavaskar, Kamaraj R.Surendiran, Dr.E.Ramaraj Technology Adviser Madurai Kamaraj University,Madurai. Three Counter Defense Mechanism for TCP SYNFlooding Attacks, International Journal of Computer Applications (0975 – 8887) Volume 6– No.6, September 2010.

[16]. Sanjyoti Tarai, Khaleel Ahmad, Jayant Sekhar PREVENTION OF SYN FLOOD DOS ATTACK International Journal of Emerging Trends & Technology in Computer Science (IJETTCS Volume 2, Issue 3, May – June 2013 ISSN 2278-6856.

[17]. G. Usha Devi*, M. K. Priyan, E. Vishnu Balan, C. Gokul Nath and M. Chandrasekhar, Detection of DDoS Attack using Optimized Hop Count Filtering Technique, Indian Journal of Science and Technology, Vol 8(26), DOI: 10.17485/ijst/2015/v8i26/83981, October 2015.

[18]. www.google.co.in/imgres