# DENIAL OF SERVICE ATTACK

# (DOS ATTACK)

Kamini[1] (MCA 2nd year)***bhartikamini177kb@gmail.com***

Mr. Deepak Kumar[2] (Assistant Professor) TMU Moradabad***deepak.computers@tmu.ac.in***

College of Computing Sciences and Information Technology.

Theerthanker Mahaveer University Moradabad.

**Abstract:-As we know that this is the age of technology and sciences' .As these all are increasing, threats related to them are also increasing one of threat is dos attack. DOS attack or distributed denial of service attack (DDoS attack) is an attempt to make a computer resource unavailable to its all users. While the means to carry out, motives for, and targets of a DOS attack may differ, it generally consists of the serious efforts of a person or people to prevent an Internet site or service from running powerfully or at all, briefly or indefinitely. DOS attack is performed by the use of botnets .For better accepting on DOS attacks, this article provides a summary on existing DOS attacks and key defence technologies in the Internet and wireless networks.**

**1. Introduction: -**Today, we are using wireless networks so the security related them has rapidly decreased.Dos attack in present is a major issue for computer networks. Denial of Service (DOS) attacks are quite new advance. These attacks was first appeared in 2000.We saw them emerge as a major new category of attack on the Internet.

A Denial of Service attack is an attempt by a person or a group of persons to attack on online service. This can have serious cost, especially for companies like Flipcart and eBay which rely on their online availability to do business. Previous single source attacks are currently countered simply by several defence mechanisms and therefore the source of those attacks will be simply rejected or blocked with improved tracing Capabilities .However, with the amazing growth of the internet throughout the last decade, an increasingly large amount of weak systems are currently available to attackers.

In this attack, attacker takes large number of computer equipment under his control over the internet and these computers are failing machines. The attacker exploits these computers weaknesses by inserting malicious code or some other hacking technique so that the machines become under his control. These compromised machines can be hundreds or thousands in numbers and these are commonly termed as 'zombies.' The group of zombies are called 'botnet'. The magnitude of attack is depends on the size of botnet, for larger botnet, attack is more vicious and vain.

Zombies of a botnet are usually recruited through the use of Trojan horses, worms, or backdoors. It is very difficult for the defence mechanisms to identify the original attacker because of the use of spoofed IP addresses by zombies under the control of the attacker with botnet.

Earlier DDoS attacks were manual, in which attacker had to implement many steps before the launch of final attack, which includes port scanning, identifying compromised machines or zombies in the internet to

**2. What is a dos attack: -** A denial-of-service attack is illustrious by an open attempt by

attackers to prevent rightful users of a service from using that service. Denial of service attack is a form of cybercrime in which attackers overload computing or network resources with so much traffic that legitimate users are unable to gain access to those resources.

**3. Risk associated to dos attack:-**In denial of service attack a hacker wants to crash our server following are the risk related to it-

i. Network bandwidth. ii. Server memory. iii. CPU usage.
iv. Hard disk space. v. Database space.
vi. Application exception handling mechanism
vii. Database connection pool.

A denial of service attack is an action that prevents or spoils the allowed use of network, system or applications by killing resources such as central processing unit (CPU).Denial-of-service attacks are considered violations of the IAB's Internet proper use policy, and also violate the acceptable use policies of virtually all Internet service providers

**4. Aims of Dos attack:-**following are the aims of dos attack:

I. Consuming bandwidth with large traffic volumes.
II. Overload or crash the network handling software.
III. Send specific type of packets to consume limited available resources.

**5. Prevention from dos attack:-**We can prevent from dos attack by the following practices:-

1. Always try to test yourself both locally and over the internet.
2. Our processes can also be harmful for us.
3. If u feel like something is wrong then ask why?
4. Protects yourself against hackers.
5. It is important to know your configurations.
6. Create interdepartmental standard operating procedures(SOPs) and Emergency Operating procedure(EOPs)

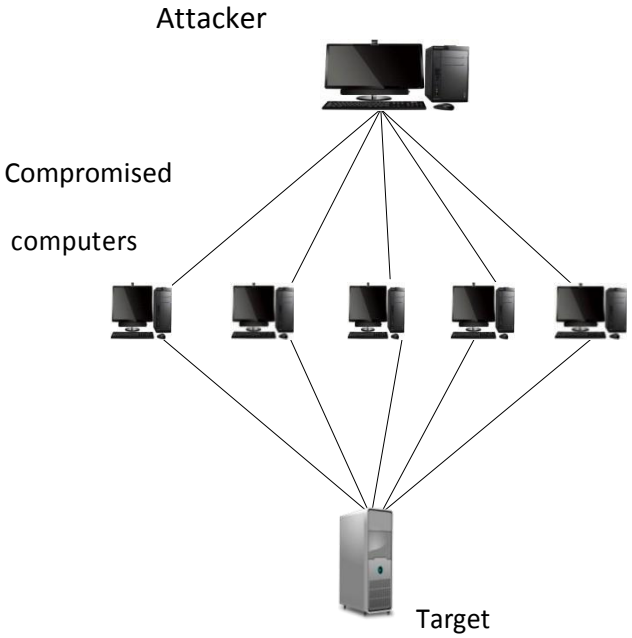


Fig.1 (DOS ATTACK)

**6. What is Distributed denial of service attack(DDOS attack)?-**A DDOS Attack organizes many machines to get this goal. The operating systems and network protocols are developed without worry security engineering which results in providing hackers a lot of insecure machines on Internet. These insecure machines are used by attackers as their crowd to launch attack. An attacker or hacker regularly inserts attack programs on these insecure machines.

A Distributed Denial of Service attack is commonly characterized as an event in which a legitimate user or organization is deprived of certain services,

like web, email or network connectivity, that they would normally expect to have. DDoS is basically a resource overloading problem. The resource can be bandwidth, memory, CPU cycles, file descriptors, buffers etc. The attackers bombard scare resource either by flood of packets or a single logic packet which can activate a series of processes to exhaust the limited resource. The figure shows that attacker uses three zombie's to generate high volume of malicious traffic to flood the victim over the Internet thus rendering legitimate user unable to access the service.

7. **How are DDoS attacks performed? -** A DDoS attack is carried out in several phases. The attacker first staffsmultiple agent machines. This process is usually performed automatically through scanning of remote machines, looking for security holes that will enable subversion.

   The discovered vulnerability is then exploited to break into recruited machines and infectthem with the attack code.

The exploit/infect phase is frequently automated, and the infected machines can be used for further recruitment of new agents. Another recruit/exploit/infect strategy consists of distributing attack software under disguise of a useful application (these software copies are called Trojans).

This distribution can be performed, for instance, by sending E-mail messages with infected attachments. Subverted agent machines are *used* to send the attack packets. Attackers often hide the identity of subverted machines during the attack through spoofing of the source address field in attack packets.

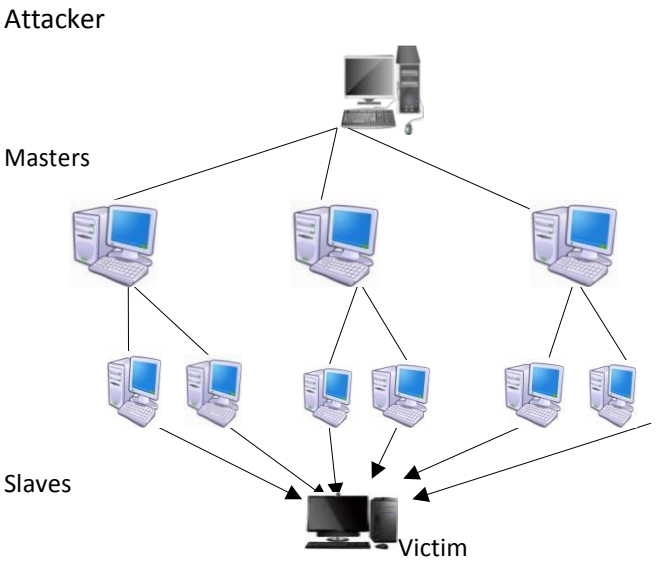


Fig 2(DDOs Attack)

**8. Types of DDoS Attack:-**

I. *SYN flood attack:-*Any system providing TCP-based network services is potentially subject to this attack. The attackers use half-open connections to cause the server

exhaust its resource to keep the information describing all pending connections. The result would be system crash or system inoperative.

II. *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.

III. *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.

**9. How to Prevent from DDOS attack: -** It isvery tough toprotect against a complicated DDoS attack launched by a gritty enemy. Dos attack can be prevent by the use of dot defender web application firewall. As dot defender inspect HTTP traffic and every packet .following are the reasons for why dot defender is good for security of network:--Many organizations struck by a DDoS are left to scramble in an effort to stop the attack once it has already begun. Sometimes this requires coordination with the ISP that provides network access. This is especially true when an ISP is forced to "null route" a victim – meaning that to protect other customers, the ISP routes traffic intended for the victim into the trash.

This of course effectively prevents all access, including from legitimate users. One of the more well-known countermeasures against a SYN flood is the use of "SYN cookies" either in the server OS or, better yet for network efficiency, in a network security device at the network edge such as the Cisco Guard. SYN cookies provide a more efficient method for tracking incoming TCP connections lessening the chance for a typical SYN flood to overwhelm the stack. The limitation with these DDoS defences is that if the attacker can generate network traffic at a higher rate than your network's Internet connection can handle, it will be

**10. Conclusion:-**

In present scenario internet reforms itself rapidly so the launching of new websites caused advanced in insecurities. Dos attack can be costly and harmful attack. The top defence is to hinder. New services are offered through the Internet, and new attacks are deployed to prevent clients from accessing these services. Still the basic issue is whether DDoS attacks represent a network problem or an individual problem—or both. If attackers are only the network problem than a plan for it must be setup through Internet protocols. If attacks are mostly the result of individual system weaknesses, the solution could derive from a successful IDS system, from an antivirus, or from an unassailable firewall. Attackers then could not compromise systems in order to create a "zombies" army.

11.**Acknowledgements**

As I write this acknowledgement, I must clarify that this is not just a formal acknowledgement but also a sincere note of thanks and regard from my side. I feel a deep sense of gratitude and affection for those who were associated with this seminar without their co-operation and guidance this seminar could not have been conducted properly .I am also indebted to my guide and friends for their constant support and their priceless reviews which helped me to take this seminar to its current level.

## References

[1]. Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, John Palfrey† The Berkman Centre for Internet & Society at Harvard UniversityDecember 2010

[2]. Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art 1Esraa Alomar, 2Selvakumar Manickam 1,2National Advanced IPv6 Centre (NAV6), Universiti Sains Malaysia, Malaysia 3,4B. B. Gupta 3University of New Brunswick, Canada 4RSCOE, University of Pune, India 5Shankar Karuppayah, 6Rafeef Alfaris 5,6National Advanced IPv6 Centre (NAV6), Universiti Sains Malaysia, Malaysia

[3]. Denial of Service AttacksQijun Gu, PhD. Assistant Professor Department of Computer Science Texas State University – San MarcosSan Marcos, TX, 78666Peng Liu, PhD. Associate Professor School of Information Sciences and Technology Pennsylvania State University University Park, PA, 16802.

[4]. Denial of Service Attack Techniques:Analysis,Implementationand Comparison Khaled M. Elleithy Computer Science Department, University of Bridgeport Bridgeport, CT 06604, USA Drazen Blagovic, Wang Cheng, and Paul Sideleau Computer Science Department, Sacred Heart University Fairfield, CT 06825, USA

[5]. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions John Bellardo and Stefan Savage Department of Computer Science and Engineering University of California at San Diego.

[6]. Distributed Denial of Service Attacks Bennett Todd <bet@oven.com>18 February 2000.

[7]. Denial of Service Attacks Qijun Gu, PhD. Assistant Professor Department of Computer Science Texas State University – San Marcos San Marcos, TX, 78666

[8]. A Study on Recent Approaches in Handling DDoS Attacks Debajyoti Mukhopadhyay1, 2 1Web Intelligence & Distributed Computing Research Lab Green Tower, C-9/1, Golf Green, Calcutta 700095, India deajyoti.mukhopadhyay@gmail.com

[9]. A Study on Recent Approaches in Handling DDoS Attacks Debajyoti Mukhopadhyay1, 2 1Web Intelligence & Distributed Computing Research Lab Green Tower, C-9/1, Golf Green, Calcutta 700095, India deajyoti.mukhopadhyay@gmail.com

[10]. ] A Review ofDDOS Attack and its Countermeasures in TCP Based Networks

[11]. Akash Mittal1, Prof. Ajit Kumar Shrivastava2, Dr. Manish Manoria3.

[12]. Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art1Esraa Alomar, 2Selvakumar Manic am 1,2National Advanced IPv6 Centre (NAV6), University Sains Malaysia, Malaysia 3,4B. B. Gupta 3University of New Brunswick, Canada 4RSCOE, University of Pune, India 5Shankar Karuppayah, 6Rafeef Affairs 5,6National Advanced IPv6 Centre (NAV6), Universiti Sains Malaysia, Malaysia