The International Journal Of Engineering And Science (IJES)
|| Volume || 5 || Issue || 5 || Pages || PP -32-35|| 2016 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

# Comparative Analysis of Different Denial of Service Attacks

[1]Anupama Khatak, [2]Raman Maini
[1]*MTech Student Department Of Computer Engineering Punjabi University, Patiala*
[2]*Professor Department Of Computer Engineering Punjabi University, Patiala*

**ABSTRACT**
*Internet connects millions of computers around the world which leads to misuse of resources too by the users and mount attacks against websites. Last year, 16 percent of the global companies were victim of the attack. Among half, websites had been hit, login were attacked in 18 per cent of the cases. One of them are DOS attacks.* ***DENIAL OF SERVICE*** *is a type of attack that originates when you ask server to process your request, so if an attacker flood the server with requests, your request cannot be processed, since server can run certain number of requests at that particular interval of time. In this work various DOS attack methods are discussed and comparison among them is done. As in ping of death small TCP/IP packets but in large number are send wherein, smurf ICMP packets are launched, buffer overflow overloads the data whereas, teardrop overlap packets. Among all these attacks PDOS are exclusive once at they completely destroy system hardware. It has been analyzed and concluded that these attacks are so effective that can either flood your system or cause destructions.*

***Keywords:*** *Attacks, Denial Of Services.*

Date of Submission: 18 April 2016 Date of Accepted: 08 May 2016

## I. Introduction

Attack is defined as an attempt to make unauthorized use of an valuable thing. It target the system which in response slow the process or stop altogether, whereas DOS attack is an attempt to make resource temporarily unavailable to their users. It is placed either by the person or the computer itself. These attacks can be intentionally or unintentionally launched. Intentionally involves planning of the hackers for criminal prosecution whereas unintentionally involves system infected with computer virus. This attack occur in two forms either flood the services or crash the services. Here, flooding means number of requests at pending state and crashing means failure of the system. DOS attacks eat up bandwidth of the system. Because of this attack, confidentiality and availability of the user is lost. This paper summarize the basics related to the denial of service attacks, methods involved in this attack and comparison derived from these attacks. In the section 2 Denial of service is explained along with methods to launch these attacks. Section 3 comprises of comparison among different types of attacks.

## II. Denial OF Service

DOS attack is an attempt to make resource temporarily unavailable to their intended user. In occurrence of this attack user is not able to access the requested site. Attacker hack the number of computers known as zombies and the attack the target computer. On the other hand, user request the server for the site which is no longer available. There are many methods one can find out to flood the system. This attack usually works by making full use of drawbacks of TCP/IP protocols. DOS attack may flood the system, may lose connection between two PC, may attempt to lose of required services like email. Dos attack is not only related to the information but also cost time and money to the companies.[3]

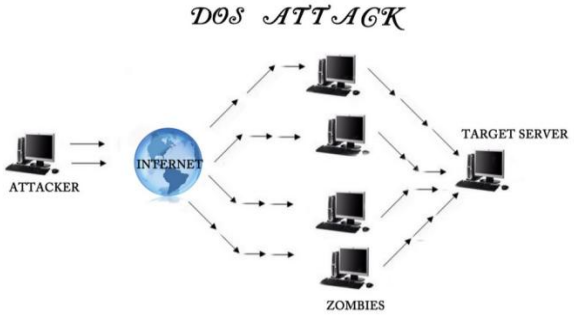


Fig:1 [2]

### *2.1 Different Type Of Attacks*

**2.1.1 Ping of death**[IV] TCP/IP allow packets as large than 65,536 bytes. Ping of death works by sending small packets in large number even more than maximum limits, hence flooding the system. Like other large but well-formed packets, this denial of service attack knowingly a ping of death is segmented into collection of eight octets before transmission[1]. However, when the target computer put together the abnormally formed packet, a buffer overflow can occur, causing a system crash and allowing the booster of noxious code of undeveloped data[1]. It has the ability to affect variety of system like unix, linux, mac, windows. Later on these attacks are overcome by firewalls. Checks are placed before reassembly of the packets so that lager packets are ignored.

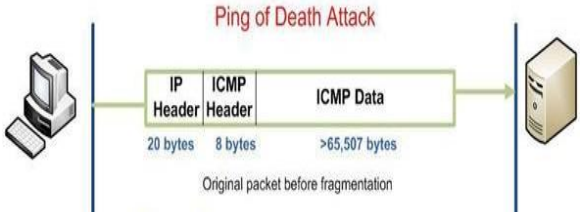


Fig:2[VI]

**2.1.2 Smurf**[IV] is basically, distributed denial of service attack. It slow down both victim network as well as network that is used to amplify the attack. In this DOS attack three fields play the major role: (a) attacker (b) victim (c) amplifier. Attacker take notice of the victim IP address, also the site that will help in amplifying the attack. Since single internet broadcast address allow maximum of 255 hosts, smurf uses large number of Internet Control Message Protocol (ICMP) packets which amplifies each ping up to 255 times. Hosts reply's to the victim network, thus slowing down the process, hence impossible to use. Smurf attacks can be avoided by configuring routers to not forward packets.

**2.1.3 Buffer Overflow**[IV] in a RAM their is temporary storage location known as buffers, it holds the data so that CPU can access it later to the disk. Buffers too have their limits to hold the data, also overwriting the same data can be the cause of the problem. Thus, this attack overloads the buffer with data, hence corrupt the data. Unlike in smurf attack, this attack can be avoided by configuring routers to not forward unwanted data.

**2.1.4 Teardrop**[IV] attack involves sending large number of packets to target machine. TCP/IP break them into fragments and are reassembled at the recovery. During recovery these packets overlap each other hence flood the system. In this IP header contains three fields (a) do not fragment bit, (b) fragment bit, (c) offset fragments. Among them focus is on fragment offsets as it states starting position of each un fragmented packets. Hacker sends fragmented offsets containing overlapped fragment offset hence floods the victims system[VI].

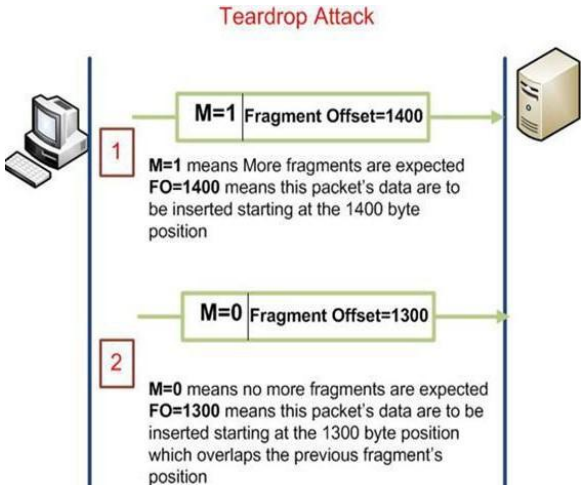


Fig:3[VI]

**2.1.5 SYN**[IV] stands for Synchronize. A SYN attack occurs when a host sends huge number of TCP/IP packets, usually with fake operators location. Each of this packets are consider a connection request, making a server to built a half-open connections, by sending in response TCP/SYN-ACK packets, thus waiting for the packets in back from sender address. Since, sender address is fake, the answer as acknowledgment never appears. Now these half-open associations penetrate the number of available associations the server can ever hold, keeping it from not letting the user to view the site requested, until attack ends [V].

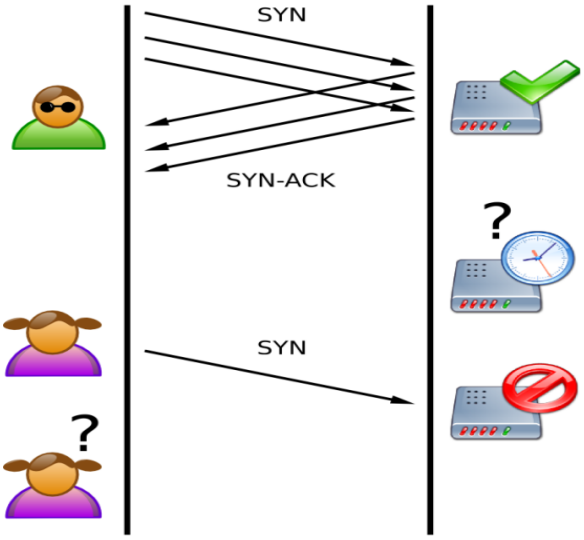


Fig:2 [V]

**2.1.6 Permanent Denial Of service attack[V]** desolate the setup so crudely that the systems hardware needs to be replaced or need to be reinstalled. They make full use of limitation related to the security of the system. Firstly, attacker replace the systems firmware with corrupted or modified firmware images thus rule the system. This is called permanent as whole system is destroyed or of no use, which require replacement of the system.

## III. Comparison Of Different Types Of Attack

| | **Ping Of Death** | **Smurf** | **Buffer Overflow** | **Teardrop** | **Synchronize** | **PDOS** |
|---|---|---|---|---|---|---|
| **Occurrence** | Sending small packets in large number. | Large number of ICMP packets. | Overloads the memory with data. | Overlap of fragmented packets during recovery. | Uses forged sender address. | Uses flaws in security of the system. |
| **Affect** | Flood and crash of the system. | Slowing down the process. | Corrupt the data. | Crash the system. | Leave half open connections. | Destroy systems hardware. |
| **Recovery** | Checks are placed to ignore large packets. | Configure routers to not forward packets. | Configure router to not forward unwanted data. | Upgrade the version. | Reducing SYN-received timers, firewalls. | Replace systems hardware. |

Table:1 Comparison Of Types Of Attacks [4] [V]

## IV. Conclusion

This paper discuss basic facts related to the denial of service attack, methods required to embed those attacks and comparison related to the attacks.

A denial of service attack can be put in motion adopting SYN flooding, Ping of Death, Teardrop, Smurf, buffer over flow or permanent denial of services. Comparison between all the six attacks are discussed and concluded that some attacks can flood the system as in ping of death, slowing of the

process as in smurf, half left open connections in SYN and worst one is PDOS which completely destroys hardware of the system. Possibly there are techniques to recover from these attacks like firewalls, routers and replacing systems hardware in case of PDOS. In the future work network stimulation tools will be used for analysis of DOS attacks.

## References


*[1]* Stephen M. Specht and Ruby B. Lee "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures." *Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550, September 2004*

*[2]* Carl, C., Kesidis, G., Brooks, R.R., and Suresh Rai. (2006,January) "Denial-Of-Service Attack-Detection Techniques" *IEEE Internet Computing, 10(1),82-89*

[3] Jelena Mirkovic, Sven Dietrich, David Dittrich, Peter Reither, "Internet Denial of Service: Attack and Defense Mechanisms", *Publisher: Prentice Hall PTR, 2004*.

[4] Santosh Kumar, Abhinav Bhandari, A. L. Sangal "Comparion of queuing algorithms against ddos attacks" *Santosh Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1574-1580*

[5] Alefiya Hussain, John Heidemann, Christes Papadopoulos "A Framework For Classifying Denial Of Service Attacks" *Conferences.signcomm.org/signcomm/2003/papers/p99.*

[6] Darin Swan University of Maryland University College "A Brief Review of Denial-of-Service-Research Papers"*academia.edu/2963956*.

*[7]* Vinko zlomislic "Denial of service attack an overview" *Information Systems and Technologies (CISTI), 2014 9th Iberian Conference.*

[8] Caballero, A. (2009). Information Security Essential For IT Managers: Protecting Mission-Critical System (chaper14). In J.R Vacca (ed.) *Computer and Information Security Handbook*. Amsterdam: Elsevier.

*[9]* Cotroneo, D., Peluse, L., Romano, S.P and Ventre, G. "An active security protocol against attacks". *Computers and Communications,2002. Proceedings.* ISCC 2002. *Seventh International symposium on Computer and Communications, Vol., no., pp. 496-501,2002.*

[10] Noble, K. (2009). "Security Through Diversity (chapter40). In J.R. Vacca (ed.) *Computer and Information Security handbook.* Amdterdam: Elsevier.


## Web References


**I.** http://people.idsia.ch/~andrea/sim/simnet.html
**II.** https://www.nsnam.org/support/faq/ns2-ns3/
**III.** http://www.isi.edu/nsnam/ns/
**IV.** ww.guru99.com/ultimate-guide-to-dos-attacks.html
**V.** https://en.wikipedia.org/wiki/Denial-of-service_attack
**VI.** http://xcessl0gycs.blogspot.in/2012/06/ping-of-death-and-other-dos-network.html