ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

A Review on Denial of Service Attacks and their Countermeasures

Indrajeet T. Zade[1], Tushar A. Rane[2]

P.G. Student, Department of Information Technology, Pune Institute of Computer Technology, Pune, India[1]

Assistant Professor, Department of Information Technology, Pune Institute of Computer Technology, Pune, India[2]

ABSTRACT:Denial of Service (DoS) attacks have become a large problem for users of computer systems connected to the Internet and normal functioning of organization causing billions of dollars of losses. Internet based network attacker can be categorized in two ways. First, Directed Denial of service attack model, where the specific Dos is developed and rolled out by an attacker with an aim to take down a specific network or computer. Second, Indirect Denial of service attack model, where a worm or virus is at large in the wild, which causes Dos and interruption as a result of its spreading. In this paper, different types of DoS and DDoS attacks and their countermeasures are reviewed. The objective of this paper is to cover many aspects of countering such attacks. This paper not only gives better understanding of DoS and DDoS attacks but also helpful to readers and researcher in identifying better defense mechanism.

KEYWORDS:Denial of Service attacks, Distributed Denial of Service attacks, classification of DDoS, defenses.

I. INTRODUCTION

Denial of Service (DoS) attacks are indeed a very serious problem in the Internet, whose impact has been well demonstrated in the computer network stream. The main objective of a DoS is the disruption of services by attempting to limit access to a host or service instead of subverting the service itself. This kind of attack focuses at rendering a network unable of providing normal service by targeting either the network's bandwidth or its connectivity. These attacks achieve their goal by sending at a victim a stream of useless packets that swamps his network or processing capacity denying access to his regular clients. In the past, there have been some large-scale attacks targeting high profile Internet sites [1], [2] and [3]. Making online services unavailable even for few minutes causes loss of revenues.

Distributed Denial of Service (DDoS), is a relatively simple, but very powerful technique to attack resources available across internet. DDoS attack is the many-to-one version of the DoS problem making the prevention and mitigation of such attacks more difficult and the impact proportionally severe. DDoS exploits the innate weakness of the Internet system architecture, its open resource access model, which amusingly, also happens to be its greatest advantage. DDoS attacks are comprised of packet streams from distinct sources. These attacks employ the power of a vast number of coordinated Internet hosts to consume some critical resource at the target and deny the service to legitimate clients. The traffic is usually so amassed that it is difficult to distinguish legitimate packets from attack packets. More importantly, size of the attack can be larger than the system can handle. Unless special care is taken, damages caused by a DDoS attack can range from system shutdown and file corruption, to total or partial loss of services.

DDoS attackers generally use different techniques and different attacking agents. Strong attacking agents include *privileged zombies*—software agents with high privileges and complete control over the machine on which they're executed, with the ability to manipulate the protocol stack, for instance, sending spoofed IP packets. Weak agents include *puppets*—programs that are downloaded automatically and run in sandboxes, such as JavaScript-based webpages. In addition, attackers might use simple types of bandwidth flooding or elaborate techniques that amplify bandwidth so uncompromised machines assist the attack [4]. There are extremely sophisticated, "user-friendly" and powerful DDoS attacking tools which have very simple logic structures and small memory sizes making them

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

relatively easy to implement and hide. Attackers constantly updates their tools to bypass security systems developed by system managers and researchers, who are in a constant alert to modify their approaches to handle new attacks.

The DDoS field is evolving quickly, thus becoming increasingly hard to grasp a global view of the problem. Although there is no elixir for all flavours of DDoS, there are several countermeasures that focus on either making the attack more difficult or on making the attacker accountable.

II. DENIAL OF SERVICE ATTACK

According to the WWW Security FAQ [5] a DoS attack can be described as an attack designed to render a computer or network unable of providing normal services. DoS attacks are being generated by a single node (or small number of nodes at the same location). The only real way for DoS attacks to impose a real threat is to exploit some software or design flaw. Such flaws can include, for example, wrong implementations of the IP stack, which crash the whole host when receiving a non-standard IP packet (for example ping-of-death)[6].The intention of these attacks compromise the availability of resources and don't necessarily damage data directly or permanently. The most common DoS attacks aim at the computer network's bandwidth or connectivity. Bandwidth attacks flood the network with such a high volume of useless traffic that all available network resources are consumed and legitimate user requests cannot get through, resulting in degraded productivity. Connectivity attacks flood a computer with such a high volume of connection requests, that all available operating system resources are consumed, and the computer can no longer process legitimate user requests.

III.CLASSIFICATION OF DoS ATTACKS

DoS attacks can be classified into five categories based on the attacked protocol level, as illustrated in Fig. 1.

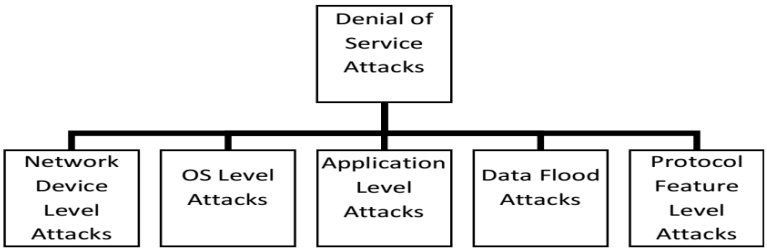

Figure 1. DoS attack types in a broader classification [7]

DoS attacks in the *Network Device Level* include attacks that might be caused either by taking advantage of bugs or weaknesses or flaws in software, or by trying to exhaust the hardware resources of network devices. One example of a network device exploit is the one that is caused by a buffer overrun error in the password checking routine. Using these exploits certain Cisco 7xx routers [8] could be crashed by connecting to the routers via telnet and entering extremely long passwords.

In the *OS level* DoS attacks take advantage of the ways operating systems implement protocols. One example of this category of DoS attacks is the Ping of Death attack [9]. In this attack, ICMP echo requests having total data sizes greater than the maximum IP standard size are sent to the targeted victim. This attack often has the effect of crashing the victim's machine.

Application-based attacks try to settle a machine or a service out of order either by taking advantage of specific bugs in network applications that are running on the target host or by using such applications to drain the resources of their victim. It is also possible that the attacker may have found points of high algorithmic complexity and exploits them in order to consume all available resources on a remote host. One example of an application-based attack is the finger bomb [10]. A malicious user could cause the finger routine to be recursively executed on the hostname, potentially exhausting the resources of the host.

In *data flooding attacks*, an attacker uses the bandwidth available to a network, host or device at its greatest extent, by sending massive quantities of data and so causing it to process extremely large amounts of data. An attacker could

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

attempt to use up the available bandwidth of a network by simply flooding the targeted victim with normal, but meaningless packets with spoofed source addresses.
DoS *attacks based on protocol features* take advantage of certain standard protocol features. For example several attacks exploit the fact that IP source addresses can be spoofed. Several types of DoS attacks have focused on DNS, and many of these involve attacking DNS cache on name servers. An attacker who owns a name server may coerce a victim name server into caching false records by querying the victim about the attacker's own site. A vulnerable victim name server would then refer to the rogue server and cache the answer [11].

IV. DISTRIBUTED DENIAL OF SERVICE ATTACKS

According to the WWW Security FAQ [5] on Distributed Denial of Service (DDoS) attacks: "A DDoS attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the DoS significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms". The DDoS attack is the most advanced form of DoS attacks. It is distinguished from other attacks by its ability to deploy its weapons in a "distributed" way over the Internet and to aggregate these forces to create lethal traffic. DDoS attacks never try to break the victim's system, thus making any traditional security defense mechanism inefficient. The main goal of a DDoS attack is to cause damage on a victim either for personal reasons, either for material gain, or for popularity. The main tool of DDoS is bulk flooding, where an attacker or attackers flood the victim with as many packets as they can in order to overwhelm the victim. The best way to demonstrate what a DDoS attack does to a web server is to think on what would happen if all the population of a city decided at the same moment to go and stand in the line of the local shop. These are all legitimate requests for service – all the people came to buy something, but there is no chance they would be able to get service, because they have a thousand other people standing in line before them. The zombie program can be planted on the infected hosts in a variety of ways, such as attachment to spam email, the latest cool flash movie, a crack to a game, or even the game itself. Communication from the zombie to its master can be hidden as well by using standard protocols such as HTTP, IRC, ICMP or even DNS [6].

V. CLASSIFICATION OF DDoS ATTACKS

A. Classification by CommunicationMechanism
Based on the communication mechanism deployed between agent and handler machines we divide semi-automatic attacks into attacks with direct communication and attacks with indirect communication [29].
Attacks with direct communication: Agent and handler communicate with each other since they know each other's identity in this case. Hard coding IP addresses of master in the attack code that is later installed agent.Each agent then reports its readiness to the handlers, who store its IP address in a file for later communication. Also, since agents and handlers listen to network connections, they are identifiable by network scanners. A Direct DDoS Attack is shown in Fig. 2

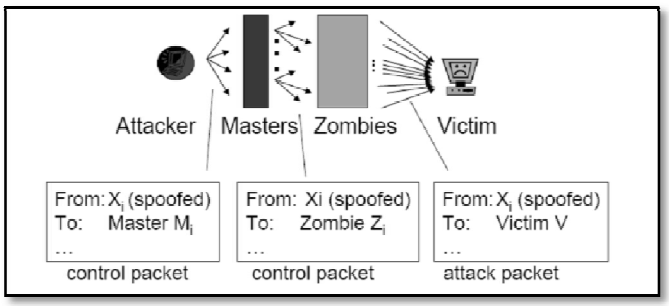

Figure2: A Direct DDoS Attack [29]

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Attacks with indirect communication: Attacks with indirect communication deploy a level of indirection to increase the survivability of a DDoS network. Recent attacks provide the example of using IRC channels [28] for agent/handler communication. The use of IRC services replaces the function of a handler, since the IRC channel offers sufficient anonymity to the attacker. Since DDoS agents establish outbound connections to a standard service port used by a legitimate network service, agent communications to the control point may not be easily differentiated from legitimate network traffic. An attacker controls the agents using IRC communications channels. A Reflector DDoS Attack is shown in Fig. 3

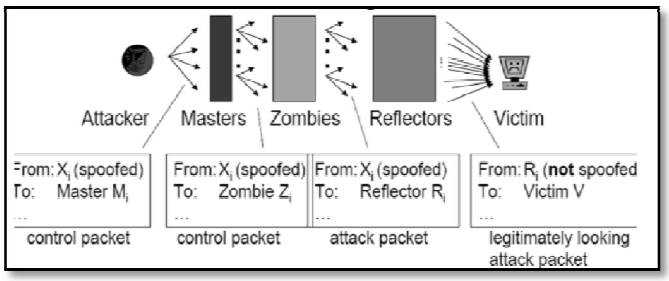

Figure 3: A Reflector DDoS Attack [29]

B. Classification by Exploited Vulnerability

Based on the vulnerability that is targeted during an attack, we differentiate between protocol attacks and brute-force attacks [29].

Protocol Attacks: Protocol attacks exploit a specific feature or implementation bug of some protocol installed at the victim in order to consume excess amounts of its resources. Examples include the TCP SYN attack, the CGI request attack and the authentication server attack.In the TCP SYN attack, the exploited feature is the allocation of substantial space in a connection queue immediately upon receipt of a TCP SYN request. The attacker initiates multiple connections that are never completed, thus filling up the connection queue indefinitely. In the CGI request attack, the attacker consumes the CPU time of the victim by issuing multiple CGI requests. In the authentication server attack, the attacker exploits the fact that the signature verification process consumes significantly more resources than bogus signature generation. He sends numerous bogus authentication requests to the server, tying up its resources.

Brute-force Attacks: A large amount of legitimate transactions is used to perform brute force attacks

Filterable Attacks: Filterable attacks use meaningless packets or packets for non-critical services of the victim's operation, and thus can be filtered by a firewall.

Non-filterable Attacks: Non-filterable attacks use packets that request legitimate services from the victim. Thus, filtering all packets that match the attack signature would lead to an immediate denial of the specified service to both attackers and the legitimate clients. Examples are a HTTP request flood targeting a Web server or a DNS request flood targeting a name server. The line between protocol and brute force attacks is thin. Protocol attacks also overwhelm a victim's resources with excess traffic, and badly designed protocol features at remote hosts are frequently used to perform "reflector" brute-force attacks, such as the DNS request attack [19] or the Smurf attack [20]. The difference is that a victim can mitigate the effect of protocol attacks by modifying the deployed protocols at its site, while it is helpless against brute-force attacks due to their misuse of legitimate services (non-filterable attacks) or due to its own limited resources (a victim can do nothing about an attack that swamps its network bandwidth).Countering protocol attacks by modifying the deployed protocol pushes the corresponding attack mechanism into the brute-force category. For example, if the victim deploys TCP SYN cookies [21] to combat TCP SYN attacks, it will still be vulnerable to TCP SYN attacks that generate more requests than its network can accommodate. It is interesting to note that the variability of attack packet contents is determined by the exploited vulnerability. Packets comprising protocol and non-filterable brute force attacks must specify some valid header fields and possibly some valid contents. For example TCP SYN attack packets cannot vary the protocol or flag field, and HTTP flood packets must belong to an establishedTCP connection and therefore cannot spoof source addresses, unless they hijack connections from legitimate clients.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

C. Classification by Degree of Automation

At the time of attack, attacker first confirms attacking agent machine where they can plant attack code.Based on the degree of automation of the attack, we categorized them as following [29].

Manual Attacks: Remote machine is scanned for vulnerabilities or weaknesses, enter into system and install the attack code, commence the attack.

Semi-Automatic Attacks: In DDoS network, there is handler (master) and agent (slave, daemon) machines. Automated script is used by attacker to scan and compromise the machines and install attack code. Attacker then uses master machine to select type of attack and victim, commencement of attack is done.

***Automatic Attacks*:** The process of attack is automated in which the time of attack, attack type, duration and victim's address are pre-programmed in the attack code. The involvement of attacker is minimum since he only issues single command where it starts attack script.

D. Classification by Random Scanning

In random scanning, compromised machine enquires random addresses in IP address space using different seed. High volume is created as many machines probe same addresses [29].

Attacks with Topological Scanning: This scanning uses compromised machine to select new targets.

Attacks with Permutation Scanning: A common pseudo-random permutation of IP address space is shared by all compromised machines. Each IP address is mapped to an index in this permutation. A machine begins scanning by using this index as starting point. If it sees already infected machines, it chooses new random start point.

Attacks with Hitlist Scanning: In hitlist scanning, compromised machine is supplied with all addresses externally. It then detects vulnerable machine, send the half of initial hitlist to recipient and keeps other half.

Attacks with Local Subnet Scanning: This scanning can be added to any of the previously described techniques to scan for targets that are connected to same subnet.

Attacks with Central Source Propagation: In this, a central server or set of servers are used as attacking agents.

Attacks with Autonomous Propagation: Autonomous propagation avoids the file retrieval step by injecting attack instructions directly into the target host during the exploitation phase.

Attacks with Back-chaining Propagation: In back-chaining propagation, compromised machine is used to download attack code and the infected machine then becomes the source for the next propagation step.

VI **DDoS COUNTERMEAUSRES**

There is no method which is sufficient to counter all kinds of DDoS attacks. There are three categories of DDoS countermeasures. First, preventing the setup of the DDoS attack network, including preventing secondary victims and detecting and neutralizing handlers. Second, dealing with a DDoS attack while it is in progress, including detecting or preventing, mitigating or stopping, and deflecting the attack. Third, there is the post-attack category involving network forensics.

A. Detect or Prevent Potential Attacks

To detect or prevent a likely DDoS attack that is being hurled, egress filtering and MIB (Management Information Base) statistics can be used. *Egress filtering* refers to the skimming of IP packet headers leaving a network and checking to see if they meet certain criteria. If the packets clear the criteria, they are routed outside of the sub-network from which they initiated. Otherwise, the packets will not be sent. Since DDoS attacks often use spoofed IP addresses, there is a good probability that the source addresses of DDoS attack packets will not represent the source address of a legal user on a specific sub-network. If the network administrator homes a firewall in the sub-network to sieve out any traffic without an originating IP address from the subnet, many DDoS packets with spoofed IP addresses will be castoff. Another method being studied to identify when a DDoS attack is occurring uses the MIB statistics from routers. Router MIB data includes parameters that indicate different packet and routing statistics. Identifying statistical patterns in different parameters during a DDoS attack [24] looks promising for possibly mapping ICMP, UDP, and TCP packet statistical abnormalities to specific DDoS attacks. Work in this area could provide methods for identifying when a DDoS attack is happening and how to adjust network parameters to compensate for the attacking traffic.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

B. Prevent Secondary Victims

One of the best methods to prevent DDoS attacks is for the secondary victim systems to prevent themselves from joining in the attack. This requires wakefulness of security issues and prevention techniques from all Internet users. To prevent secondary victims from becoming infected with the DDoS agent software, these systems must continually observe their own security. They must ensurethat no attack code have been installed on their systems and make sure they are not indirectly sending agent traffic into the network. Because the Internet is so dispersed, with so many different hardware and software platforms, it is difficult to find proper function. To be successful, end users must have the resources to meet the expense of protective measures and the information to choose the right protections. Additionally, secondary victims must identify when they are joining in a DDoS attack, and if so, they need to know how to halt it. These tasks are daunting for the average "web-surfer". Recent work has proposed built-in mechanisms in the core hardware and software of computing systems that can provide defenses against malicious code insertion through buffer overflow violations [22]. This can significantly reduce the probability of a system being compromised as a secondary victim for a DDoS attack. Another strategy is for network service providers and network administrators to add dynamic pricing to network usage, to encourage secondary victims to become more active in preventing themselves from becoming part of a DDoS attack. If providers chose to burden differently for the use of different resources, they would be better able to identify legitimate users. This system would make it easier to prevent attackers from entering the network [23]. Additionally, secondary victims who might be charged for accessing the Internet may become more aware of the traffic they send into the network and hence may do a better job of regulating themselves to verify that they are not participating in a DDoS attack.

C. Detect and Neutralize Handlers

Detecting and neutralizing handler is important method for mitigating DDoS attacks. Learning communication protocols and traffic patterns between handlers and clients or handlers or agents, is a technique to identify network nodes that might be infected with handler code. Since there are far less DDoS handlers deployed than agents, shutting down a few handlers can render multiple agents useless thereby neutralizing a DDoS attack.

D. Deflect Attacks

An Internet-attached server that acts as a decoy, luring in potentialhackers in order to study their activities and monitor how they are able to break into a system. Honeypots are designed to mimic systems that an intruder would like to break into but limit the intruder from having access to an entire network. If a honeypot is successful, the intruder will have no idea that s/he is being tricked and monitored. Most honeypots are installed inside firewalls so that they can better be controlled, though it is possible to install them outside of firewalls. A firewall in a honeypot works in the opposite way that a normal firewall works: instead of restricting what comes into a system from the Internet, the honeypot firewall allows all traffic to come in from theInternet and restricts what the system sends back out [26].

E. Post-Attack Forensics

If *traffic pattern* data is stored during a DDoS attack, this data can be examinedpost-attack to look aimed at specific characteristics within the attacking traffic. This characteristic data can be used for updating load balancing and throttling countermeasures to intensify their efficiency and protection ability. Additionally, DDoS attack traffic patterns can help network administrators develop new filtering techniques for preventing DDoS attack traffic from entering or leaving their networks. To help identify the attackers, *packet traceback*techniques are proposed [27]. The concept involves tracing internet traffic back to its source (rather than that of a spoofed source IP address). This technique helps to detect the attacker. Additionally, when the attacker sends different types of attacking traffic, this method supports in providing the victim system with information that might help develop filters to block the attack. A model for developing a Network Traffic Tracking System that would identify and track user traffic throughout a network has been proposed [28]. This model can be very successful within a closed network environment where internal client systems can be fully managed by a central network administrator who can track individual end-user actions. This method begins to break down over widely distributed networks [28]. Network administrators can also keep *event logs* of the DDoS attack information in order to do a forensic analysis and to assist law enforcement in the event the attacker does severe damage. Using Honeypots and other network equipment such as firewalls, packet sniffers, and server logs, providers

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

can store all the events that occurred during the setup and execution of the attack. This allows network administrators to discover what type of DDoS attack (or combination of attacks) was used.

F. Mitigating the Effects of DDoS Attacks

Throttling is another technique proposed to prevent servers from going down. The Max-min Fair server-centric router throttle method [25] sets up routers that access a server with logic to adjust (throttle) incoming traffic to levels that will be safe for the server to process. This can prevent flood damage to servers. Additionally, this method can be extended to throttle DDoS attacking traffic versus legitimate user traffic for better results. This method is still in the experimental stage, however similartechniques to throttling are being implemented by network operators. The difficulty with implementing throttling is that it is hard to decipher legitimate traffic from malicious traffic.

Load balancing can improve both normal performance as well as lessen a DDoS attack. Network providers can increase bandwidth on critical connections to avert them from going down in an attack. Additionally, providers can duplicate servers and provide additional guaranteed protection if some go down during a DDoS attack.

VII. LITERATURE REVIEW

The Internet is susceptible to denial-of-service (DoS) attacks, where inmany hosts send a huge number of packets to cause congestion and interrupt legitimate traffic. So far, DoS attacks have engaged relatively crude, inefficient, brute-force mechanisms; future attacksmight be meaningfully more effective and harmful. To meet the increasing threats, more advanceddefenses are necessary [4].Christos Douligeris and Aikaterini Mitrokotsa [29] present structural approach to the DDoS problem by developing a classification of DDoS attacks and DDoS defense mechanisms.Sílvia Farraposo,Laurent Gallon and Philippe Owezarski [6] gave detail steps of how to launch DoS attacks and how protocols are being manipulated by these attacks. Various tools used to carry out attacks are also discussed. Moti Geva, Amir Herzberg, and Yehoshua Gev discuss bandwidth distributed denial of service attacks and response mechanisms to counter such attacks [4]. Mohd. Jameel Hashmi, Manish Saxena and Dr. Rajesh Saini give overview of DDoS tools that are used to launch attacks [30].

TABLE I
COMPARISON OFSOME OF DEFENSE MECHANISMS

Sr. No.	Defense Mechanisms	Description
1.	Ingress/Egress filtering at source's edge router	Detect and filter packets with spoofed IP addresses at the source's edge routers based on the valid IP address range internal to the network [31].
2.	Packet marking and filtering mechanisms	Mark legitimate packets at each router along their path to the destination so that victims" edge routers can filter the attack traffic.
3.	IP Traceback mechanisms	Traces back the forged IP packets to their true sources rather than the spoofed IP addresses [34].
4.	SYN Cache	Effective because the secret bits prevent an attacker from being able to target specific hash values [35].
5.	SYN Cookies	SYN cookies modify the TCP protocol handling of the server by delaying allocation of resources until the client address has been verified [35].
6.	Firewalls and Proxies	Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses [35].
7.	IP level defense mechanism	These defense mechanisms are used as countermeasure to IP-Level DDoS attacks.
8.	Mitigation on the page access behavior	Prevent HTTP-GET flooding attacks.
9.	D-WARD	Stop attack traffic originating From a network at the border of the source network [32].
10.	MULTOPS	Detects and filters DDoS flooding attacks based on significant difference between the rates of traffic going to and coming from a host or subnet.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

VIII. CONCLUSION

Denial of service and distributed denial of service attacks which exploit weaknesses in the design and architecture of internet pose a serious threat not only to wired network but also wireless infrastructures. There are many sophisticated and easy to use tools to conduct such attacks. Day by day attackers update these tools to launch DoS and DDoS attacks against individual Web sites, chat servers, email servers or network components such as aggregation routers, core routers or DNS servers. These attacks cannot be completely up-rooted but true efforts are made to mitigate them.
This paper tries to give clear view of DoS and DDoS attack and numerous defense solution that have been proposed. By getting this clear view of problem, more effective solutions to these attacks can be found.

REFERENCES

[1] CERT Coordination Center, Denial of Service attacks, Available from http:// www.cert.org /tech_tips/denial_of_service.html.
[2] Computer Security Institute and Federal Bureau of Investigation, CSI/FBI Computer crime and security survey 2001, CSI, March 2001, Available from <http://www.gocsi.com>.
[3] D. Moore, G. Voelker, S. Savage, Inferring Internet Denial of Service activity, in: Proceedings of the USENIX Security Symposium, Washington, DC, USA, 2001, pp. 9–22.
[4] M. Geva, A. Herzberg and Y. Gev, "Bandwidth Distributed Denial of Service: Attacks and Defenses", IEEE Security & Privacy, vol. 12, no. 1, pp. 54-61, 2014.
[5] L.D. Stein, J.N. Stewart, The World Wide WebSecurity FAQ, version 3.1.2, February 4, 2002, Available from http:// www.w3.org /Security/Faq.
[6] Sílvia Farraposo, Laurent Gallon, Philippe Owezarski, "Network Security and DoS Attacks",April 2005.
[7] D. Karig, R. Lee, Remote Denial of Service Attacks and countermeasures, Department of Electrical Engineering, Princeton University, Technical Report CE-L2001-002, October 2001.
[8] CIAC, Information Bulletin, I-020: Cisco 7xx password buffer overflow, Available from http://ciac.llnl.gov/ciac/bulletins/i-020.shtml.
[9] Kenney, Malachi, Ping of Death, January 1997, Available from http:// www.insecure.org /sploits/ping-o-death.html.
[10] Finger bomb recursive request, Available from http:// xforce.iss.net/static/47.php
[11] D. Davidowicz, Domain Name System (DNS) Security,1999,Available from http://compsec101.antibozo.net/papers/dnssec/dnssec.html.
[12] CERT Coordination Center, "Code Red II," http://www.cert.org/incident_notes/IN-2001 09.html.
[13] CERT Coordination Center, "Nimda worm," http://www.cert.org/advisories/CA-2001-26.html.
[14] CERT Coordination Center, "Trends in Denial of Service Attack Technology," October 2001.
[15] CERT Coordination Center, "Ramen worm," http://www.cert.org/incident_notes/IN-2001 01.html.
[16] K. Hafner and J. Markoff, Cyberpunk: Outlaws and hackers on the computer frontier, Simon & Schuster, 1991.
[17] CERT Coordination Center, "Code Red," http:// www.cert.org/incident_notes/IN-2001 08.html
[18] N. Weaver, "Warhol Worm, "http:// www.cs.berkeley.edu/~nweaver/warhol.html.
[19] CERT Coordination Center, "DoS using nameservers,"http://www.cert.org/incident_notes/IN-2000-04.html.
[20] CERT Coordination Center, "Smurf attack," http://www.cert.org/advisories/CA-1998-01.html
[21] CERT Coordination Center, "TCP SYN flooding and IP spoofing attacks," http:// www.cert.org/advisories /CA-1996-21.html.
[22] Ruby Lee, David Karig, Patrick McGregor and Zhijie Shi, "Enlisting Hardware Architecture to Thwart Malicious Code Injection", Proceedings of the International Conference onSecurity in Pervasive Computing (SPC-2003), LNCS 2802, pp.237-252, Springer Verlag, March 2003.
[23] David Mankins, Rajesh Krishnan, Ceilyn Boyd, John Zao, and Michael Frentz, "Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing", Computer SecurityApplications Conference, 2001. ACSAC 2001. Proceedings 17thAnnual, pp. 411-421, 2001.
[24] Joao B. D. Cabrera, Lundy Lewis, Xinzhou Qin, Wenke Lee, Ravi K. Prasanth, B. Ravichandran, and Ramon K. Mehra,"Proactive Detection of Distributed Denial of Service Attacks Using MIB Traffic Variables – A Feasibility Study", IntegratedNetwork Management Proceedings, pp. 609 622, 2001.
[25] David K. Yau, John C. S. Lui, and Feng Liang, "Defending Against Distributed Denial of Service Attacks with Max-min Fair Server-centric Router Throttles", Quality of Service, 2002 Tenth IEEE International Workshop, pp. 35-44, 2002.
[26] Webopedia.com, "What is honeypot? A Webopedia Definition", 2015. [Online]. Available:http://www.webopedia.com/TERM/H/honeypot.html.[Accessed: 30- Dec- 2015].
[27] Vern Paxon, "An Analysis of Using Reflectors for Distributed Denial of Service Attacks", ACM SIGCOMMComputer Communication Review, Vol. 31, Iss. 3, Jul 2001.
[28] Thomas E. Daniels and Eugene H. Spafford, "Network Traffic Tracking Systems: Folly in the Large?", Proceedings ofthe 2000 Workshop on New Security Paradigms, Feb. 2001.
[29] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art", Computer Networks, vol. 44, no. 5, pp. 643-666, 2004.
[30] Mohd. Jameel Hashmi1, Manish Saxena2 and Dr. Rajesh Saini ,"Classification of DDoS Attacks and their Defense Techniques using IntrusionPrevention System"International Journal ofComputer Science & Communication Networks,Vol 2(5), 607-614.
[31] P. Ferguson, P. Ferguson, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing"
[32] JelenaMirkovi´c Gregory Prier Peter Reiher, "Attacking DDoS at the Source".
[33] ZeeshanShafi Khan, Nabila Akram, Khaled Alghathbarl, Muhammad She, RashiMehmood, "Secure Single Packet IP Traceback Mechanism to Identify the Source".
[34] Tools.ietf.org, "RFC 4987 - TCP SYN Flooding Attacks and Common Mitigations", 2015. [Online]Available:http://tools.ietf.org/html/rfc4987. [Accessed: 31- Dec- 2015].