IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 4 (Jul. - Aug. 2013), PP 57-62
www.iosrjournals.org

A Comparative Approach to Handle Ddos Attacks

Aaruni Goel[1], Anirudh Kumar Tripathi[2], Paresh Pathak[3]
[1,2,3]*(I.T Department,IIMT Engineering College, India)*

Abstract: *Denial of Service Attacks basically means denying valid Internet and Network users from using the services of the target network or server. It basically means, launching an attack, which will temporarily make the services, offered by the Network unusable by legitimate users. In others words one can describe a DOS attack, saying that a DOS attack is one in which you clog up so much memory on the target system that it cannot serve legitimate users. Or you send the target system data packets, which cannot be handled by it and thus causes it to either crash, reboot or more commonly deny services to legitimate users. In this paper we focus on the cause and severity caused by some of the major types of DoS/DDos attacks and their countermeasures.*

Keywords: *TCP/IP, Zombies, Flooding, UDP, Ingress Routers, Engress Routers, Botnets, IP Spoofing, Firewalls, Intrusion Detection and prevention system.*

Submitted date 18 June 2013 **Accepted Date: 22 June 2013**

I. Introduction

A Denial-of-service attack (DoS attack) is a type of Computer/network attack in which a malicious hacker or a teen experiment formulates the computer or network resource unavailable to the genuine user(s). This typically includes the assault on websites, dedicated web-servers like those of intelligence , Government sites, banking systems and so on to gain either access or make unavailable the necessary resources. The types of DoS not only attack the intended host but also the complete network.

In Distributed Denial of Service many zombies use to attack to a single system. A zombie is a computer infected by Trojans by hacker to gain full control on these systems. Hackers with the help of these controlled massive systems perform many DoS attacks. Thus the attack is termed as distributed attacks like SYN flooding, UDP flooding, ICMP flooding attacks etc. on the targeted victims.

1.1 Deadly Impacts

The Attacks which primarily concern effect the performance of computers, but not limited to[1],[2]:

- The utmost CPU utilization causes the very slow performance of computer or to prohibit system to work-out on any assignment.
- Errors are generated in executing the instructions sequence wise so that the computer enters into a ‘Hang’ state.
- Operating System/Softwares bugs and vulnerabilities are utilized by these attacks and so resource allocation and other deficiencies come into picture. For example –errors in log files, Physical memory consumption, break down or shut down of Operating System itself.

The Attacks which in general further devastate networks are:

- The performance of network becomes very time consuming.(for example during internet access)
- The unavailability of a particular web site
- A high shoot up in receiving large number of E-mails through E-mail Bombs i.e the Spam Mails.

II. Types Of Attacks (Ddos/Dos) And Countermeasures

Basically the DDoS attacks are based on flooding of request packets. In this paper we only discussing some popular but defamed DDoS attacks methodologies which are mentioned in the following subsections:

a. SYN Scanning (Half-open) and/ or SYN Flooding :

This is accomplished by SYN scanning technique. In this process a hacker use to conclude the status of every communications port without establishing a full connection through TCP/IP pretending the connection establishment by three way handshaking process. In three way handshaking the user sends a SYN packet to the server which in response replies with SYN/ACK packet [3]. After receiving this SYN/ACK packet the client sends ACK packet again to the server which results the three way handshaking connection establishment. the It works as hacker sends SYN packet to show that he is eager to communicate. In reply the server sends the

SYN/ACK packet from a port to show that server is also willing to make connection establishment. Now hacker sends RST packet which results that server guess that any type of communication error (for the same reason half open term is used). Since the port on server side is still open so it is susceptible for exploitation and can get access to server files. It should be noted that if server sends a RST packet then it means the port from server side has been closed and could not be abused.

In case of SYN flooding a fake IP address is used (IP Spoofing) which is valid one. A hacker then sends a large number of SYN packets (floods) packet to server very frequently. In this scenario, server responds with SYN/ACK packets to that IP which was already spoofed by fake person. It consumes the server resources in terms that the server allocates the memory buffer for the pending connection and wait and thereby the degradation of bandwidth . Since there is always timeout period for these connections but the associated problem is that a malicious intension person can send large number of SYN packets if he has fast internet connection before the pending timeout ends.

Precautionary Steps

- Always install the latest security patches related to Operating Systems, Antivirus, Browsers .
- Always purchase certified licensed softwares.
- One way is to alter the TCP/IP networking of operating system. By this one can increase the size of the memory buffer queues and reduce the timeout values, increasing the targeted system's resistance to the attacks and using the methods for capturing packets coming from spoofed IP address by installing Ingres router filters[4] .

b. UDP Flood

A UDP flood attack is accomplished by taking undue advantage of User Datagram Protocol (UDP) which is a connectionless protocol unlike Transmission Control Protocol (TCP) and also works in Transport layer. Since UDP is a connectionless protocol so no handshaking is required in connection establishment between source and the destination. This makes the situation more critical. It is so because in this attack server has to receive every UDP packet for communication. During flooding of these packets to arbitrary ports makes the server response 'Unreachable Destination' through large number of ICMP packets continuously. This makes the genuine service which is trying to access the attacked system is averted[1],[6].

The prime attacker may also hide his identity by IP address Spoofing which results that return path of ICMP will not return to the zombies but instead they will be redirected to spoofed Address.

NewTear, Newtear2, Bonk, and Boink are the name of few attacks that finds the UDP flooding vulnerabilities in the Microsoft Windows 9.x/NT. In these attacks destination receives deformed IP fragments which get reassembled into an invalid UDP datagram which results the 'Blue Screen Of Death' at destination. The operating system may crash or need to be rebooted but unsaved tasks cannot be rescued.

Precautionary Steps[3]

- Always use firewalls in a network which is used to filter the incoming or outgoing network data traffic by using the pre-specified rules.
- Justifiable traffic should be only permissible through UDP port 53 (DNS).
- Update system with licensed only certified softwares.
- Usage of Ingress/Egress router filtering

c. ICMP Flood

ICMP flood attack sometimes is also identified by other names such as a ping of death attack, ping flood or Smurf attack. Basically Ping is a command which is used to check the availability of any host in Computer networks. If that particular machine is not available then a message comes like 'unreachable host. If the machine is on the network then output of ping command gives four fields [11] –(a) IP Address of destination machine for whom command is launched. (b) Size of packet sent by this command using Internet Control Message Protocol (ICMP) also coined as echo request packets of 32 bytes (since IPv4 address is of 32 bytes). (c) Round-trip time delay in milli-seconds for messages sent and (d) Time to Live (TTL) i.e. Life of sent packet. But this command is also used for ICMP flooding in the following manners:

2.3.1. Ping flood: It is the technique by which tremendous amount of Ping (echo request) packets are sent victim without waiting for answer back which results in crushing the band width of attacked computer. It is most frightful in the scenario if attacker has high bandwidth line then victim. It is due to the fact that the response of victim in terms echo reply packets will be too much delayed due to consumption of near about all of its bandwidth. Further the condition will be extremely worst if processing CPU speed of attacked computer is also slow.

2.3.2 Ping of death: In this method over sized ICMP packets are sent to target computer. Here oversized means that the ping packet size is greater than maximum IPv4 packet size, which is 65,535 bytes. It should be noted that ping is usually of 32 bytes or at maximum of 84 bytes if considering Internet Protocol [IP] header. But flooding of these ping packets collapsed the TCP/IP stack of the targeted machines which in reaction stop responding to TCP/IP requests. This happening ultimately crash the system of sufferer.

2.3.3. Smurf Attack: The most dangerous DDoS attack which occurs due to misconfiguration of network routers. In it the attacker sends a huge number of echo request packets. It is to be noted that IP spoofing is done here in such a way that spoofed source IP address is the targeted host. Due to miscofiguration of routers all the ping requests are transferred to broadcast address of network which results all the present hosts in the network will receive this request and give echo replies to the spoofed address of the victim [6]. If network is quite large then this will ultimately consume all the bandwidth of victim whose address has been spoofed for echo request purpose. Such type a used network is also termed as Smurf amplifier.

Precautionary Steps[3]

- Every host and routers should be so configured that they should not answer the ping calls through broadcasts.
- The routers must be so configured that do not forward packets which intended for broadcast addresses.
- Ingress/Egress router should be used which discards spoofed IP address packets.
- Smurf Amplifier registry should be consulted which is the blacklisted list of those networks that are used for Smurf attacks knowingly or unknowingly.

d. Teardrop Attack

This type of attack happens when a garbled IP packet reaches at destined target. It simply handles the overlapping of fragmented payload during reassembly of IP packet at destination. Many softwares like Nmap, Nessus etc. are used to create such garbled packets. In this attack the header of IP is tampered. Along with other different fields IP header has three fields that deal with fragmentation and reassembly of IP datagram and are [8]:

- Do not fragment (1 bit): If the value of this field is 0 then datagram can be fragmented. If sets to 1 then in this datagram no fragmentation is allowed machine must not fragment the datagram. Further if machine is not able to pass this datagram due to unavailability of required physical network, it discards the datagram and ICMP error message is sent to the source.
- More fragments (1 bit): If value is 1 then datagram is not the last fragment i.e. more fragments are expected. If its value is 0, it then it is either last or the only fragment.
- Fragment Offset (13 bits): Specifies the relative position of particular fragment with respect to its datagram and measured in units of 8 bytes.

In this attack the Fragment Offset field is often tampered. A fragmented offset IP packet is passed which contains the overlapped Fragment Offsets. When this packet reaches to the destined target then it is just impossible to reassemble them and this drain off attacked machine resources. These attacks crashed many earlier versions of Windows and Linux based operating system.

Precautionary Steps:

- The careful analysis of packets is done to identify whether any alteration in offset field using sniffers.

2.4 Land Attack

It is another type of attack in which the attacker in its move exercises a SYN Flood attack by using the source and destination IP address of the targeted machine. This result the victim’s machine falls into infinite loop in order to complete the TCP connection till the timeout period and the machine will either crash or all its CPU resources will be weakened. This attack is vulnerable for both Windows and Linux Operating systems.

Precautionary Steps [3]

- All incoming packets should be carefully analyzed with the help of Router and Firewalls rule who pretending themselves that they are coming from internal network.
- The latest Service Patches should be installed.
- Service provider should use and provide ingress filtering.

2.5 **Win Nuke**

This type of attack is done when attacker sends Out-of-Band (OOB) data to targeted victim. Basically OOB is a urgent pointer in TCP/IP. It is that part of data stream that if the value of URG pointer of bit is set is in TCP/IP segment, then a separate 16 bits is valid and used when the segment contains urgent data. It is the number that to be added to the sequence number of TCP/IP segment to obtain the number of the last urgent byte in the data section of the segment. In this way urgent data is identified which informs the machine that this separate urgent stream other than main stream is of utmost importance and must be processed first then main data stream. The attacker launches a Win Nuke program and gets connected through port 139(NETBIOS). It should be noted that other open ports are also likely to be susceptible due to this attack[11] . In this scenario OS is not able handle tackle properly and results Blue Screen of Death. But only good thing is that only unsaved information is lost, all the svae data remain unchanged. This DoS attack affects Windows 95, NT and 3.11 machines.

Precautionary Steps [3]:

- Check firewalls settings
- Update antivirus with latest security patches

2.6 Naptha

It quite works similarly to SYN flood attack but is one step ahead and works on the half-lose mechanism of TCP/IP.

As like SYN flood attacker transmits SYN packets to the targeted system with forged IP address. Now if the targeted system wants to close the system it will have to send FIN request to client (attacker) and goes to FIN WAIT-1 state. This connection remains open until the time out or if attacker does not send ACK reply for which he doesn't respond. The case becomes dramatically erroneous for systems when this attack is launched through multiple zombies

The vulnerability affects a wide variety of operating systems, like Windows9x, Windows NT (both Microsoft), HP-UX (Hewlett-Packard), Solaris (Sun Microsystems), Linux and FreeBSD (free, open and non-commercial operating systems).

Precautionary Steps [3] :

- Usage of egress and ingress filtering at network border to reduce IP spoofing.
- Firewall or routers should be configured to prevent unsuitable IP addresses
- Check and stop suspected listening services to wipe out attackers.
- Scan systems for Trojans.
- Log files should be checked for any suspicious activity.
- Check CPU utilization .

III. Brief Discussion on DDoS Activities

Recent DDoS Statistics: M. Robertson et al. [1], expressed their views by saying that approximately 2000-3000 DDoS attacks per week are occurring. Further every time the pattern of these attacks is update of previous one. The analysis revealed the fact that in over three year period that around 68,700 attacks are done on 34,700 distinct internet users of different organizations. Further the data comes from Prolexic's DD0S Report for the first quarter of 2013 stated that the average attack bandwidth totaled 48.25 Gbps in first quarter of 2013, a 718 percent increase over last quarter. Fig.1 elaborates that due to different cyber attacks how much financial loss has to be tolerated by world per year. This report also suggests that this loss will significantly be increased every year. Recently the attackers has designed 'itsoknoproblembro' toolkit which is a type of PHP script injected into targets system. It results that attacker upload and execute any Perl script on remotely compromised system resulting DDoS attack. It is so because this script is used to inject an encrypted payload. By this way it just bypass Intrusion Prevention System or antivirus protection at conquer over file index.php of website. Thereby an attacker loads Perl script any time for completion of his malicious intension.

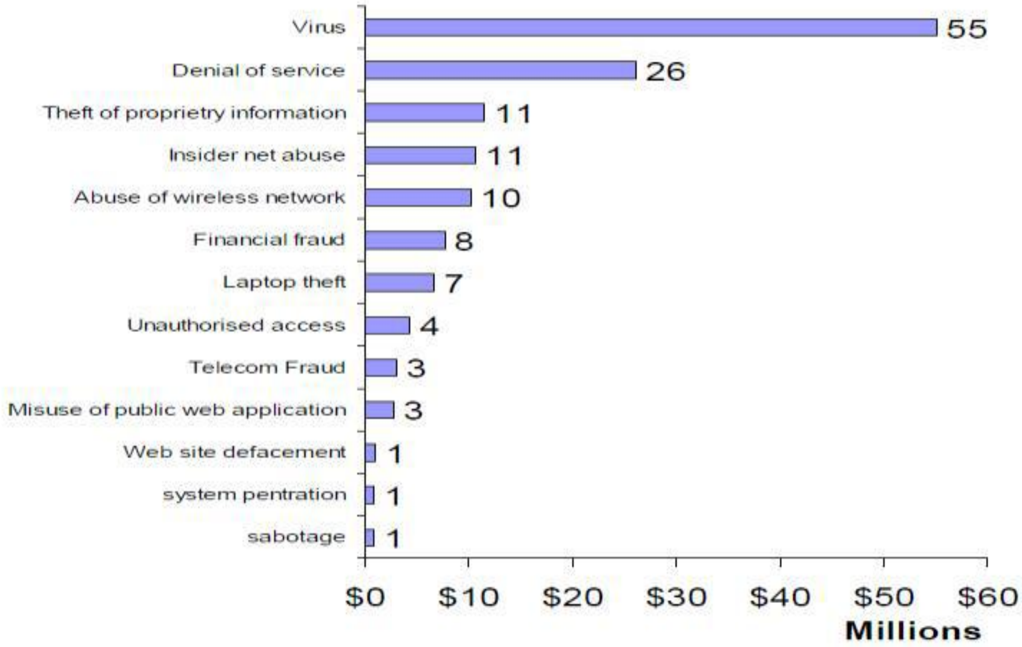

Fig. 1

Combating Platforms: For combating DDoS attacks various emulation techniques have been developed. This techniques just provide the testbeds for DDos attacks countermeasure. Few popular of them are Emulab [8], DETER [9] and Planetlab [10]. Usage of Emulab and DETER platform give users, for testing purpose, to access to number of computers which are on LAN and separated from internet. By this way the nature of attack is analyzed and experts develop the countermeasures against DDoS attacks. Planetlab is a distributed testbed where participating organizations contribute machines. Users gain shared access to those machines via virtual machine software that achieves user isolation. They can organize Planetlab nodes into overlays — traffic between nodes travel son the Internet and experiences realistic delays, drops and interaction with cross-traffic. Users can also install applications on Planetlab nodes, but their choice of OS and their privileges on nodes are much more limited than in Emulab or DETER.

It should be noted that the impact of DDoS attacks can be reduced but not restricted if the configuration of firewalls, routers and Intrusion detection and prevention system are finely tuned. CERT also suggests if problem still persists then one should check mailing lists such as bugtraq or should contact his vendor [12].

Symantec Security Response [13] encourages all users and administrators to adhere to the following basic security "best practices":

- One should turn off needed services, such as an FTP server, telnet, and a Web server. These services are heaven for attackers of attack.
- On the compromised network, all the network services should be disabled before applying the new security patch.
- The patch/security update should always be up-to-date. This could be done by visiting trusted security bulletins websites or by using vendor's latest instruction on security.
- Using complicated passwords it is quite difficult to break password files by using brute force techniques. This helps to prevent or limit damage when a computer is compromised.
- Mail server should be so configured that it either block or remove virus or Trojan infected attachments like- .vbs, .bat, .exe etc..
- Emloyees should be trained regularly about the cyber threats.
-

IV. Conclusion

According to Douligeris et al. [11]: Prevention, Detection and Characterization, Traceback, and Tolerance and Mitigation are the strategies which can prevent DDoS attacks. As we have seen the major problem of all DDoS floods is due to vulnerability of TCP/IP suite which is the backbone of internet. Microsoft Internet Security and Acceleration (ISA) Server, Nexusguard, Riorey are the major players which provide Anti Dos solutions. Organizations specially network administrators should aware that what the loss of cost they would bear if DDos attack on their server in near future. It is so because Network administrators generally think that their network is safe if they configured their firewalls and intrusion Prevention Systems. A survey conducted by Neustar that and found that only 3% organization covered in its survey has Anti Dos solution. The one way if an organization not buys costly DDoS solution for any reason or otherwise then it should define the maximum limit of data transfer from its web server to internet. At the last but not the least the war is still going and will be continued as new DDoS attacks are constantly being dreamed up by hackers by finding out more vulnerability.

References

[1] M. Robinson, J. Mirkovic, M. Schnaider, S Michel, P. Reiher, "Challenges and principles of DDoS defense", SIGCOMM 2003.

[2] K. Kumar, R.C. Joshi, K. Singh, "An Integrated Approach for Defending against Distributed Denial-of-Service (DDoS) Attacks", IRISS, 2006, IIT Madras.

[3] Reeta Mishra, Amit Asthana, Jayant Shekhar,"Distributed Denial of Service Attacks Prevention,"VSRD-IJCSIT, Vol. 1(1), 2011,pp 1-8.

[4] Global Incident analysis Center–Special Notice–Egress filtering, [Online] Available: <http://www.sans.org/y2k/egress. htm>

[5] K. Park, H. Lee, "On the effectiveness of route-based packet filtering for Distributed DoS attack prevention in power law Internets", in Proceedings of the ACM SIGCOMM 01Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press, New York, 2001, pp. 15–26.

[6] T. Bullot, R. Khatoun, L. Hugues, D. Gaïti, and L. Merghem-Boulahia. A Situatedness Based Knowledge Plane For Autonomic Networking. *ACM International Journal of Network Management, special issue on NGN*, 18(2):171–193, April 2008.

[7] C. Green and M. Roesch. Snort users manual 2.8.0 - the snort project. Technical report, Aout 2007.

[8] White, B., Lepreau, J., Stoller, L., Ricci, R., Guruprasad, S., Newbold, M., Hibler, M., Barb, C. and Joglekar, A., An Integrated experimental environment for distributed systems and networks. In Proceedings of the Fifth Symposium on Operating Systems Design and Implementation (OSDI02), (Dec. 2002). Pp 255-270.

[9] Benzel, T., Braden, R., Kim, D., Neuman, C., Joseph, A., Sklower, K., Ostrenga, R. and Schwab, S., Experience with DETER: A Testbed for Security Research. In Proceedings of Tridentcom, March 2006.

[10] Peterson, L., Bavier, A., Fiuczynski, M.E. and Muir, S. "Experiences building planetlab." In Proceedings of the 7th USENIX Symposium on Operating System Design and Implementation (OSDI '06), Seattle, WA, November 2006.

[11] Douligeris C. and Mitrokotsa, A., DDoS Attacks and Defense Mechanisms: Classification and State of the Art," Computer Journal of Networks, vol. 44, no. 5, pp. 643-666, 2004