Journal of Information and Operations Management
ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-136– 140
Available online at http://www.bioinfo.in/contents.php?id=55

DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS - CLASSIFICATION AND IMPLICATIONS

ABHISHEK JAIN AND ASHWANI KUMAR SINGH

Department of Computer Science, Graphic Era University, Dehradun, India
*Corresponding Author: Email- abhishekmbd@rediffmail.com

Received: December 12, 2011; Accepted: January 15, 2012

Abstract- Denial of Service (DoS) attacks are in place since a long time and they pose a real threat to various Internet Services. They are characterized by the method used and damaged caused particularly in case of Distributed Denial of Service (DDoS) attack. This paper presents the problem of DDoS attacks, a selective survey of various types of DDoS attacks and also gives broad classification of defense mechanisms based on various criteria. The aim of this paper is to provide a better understanding of DDoS problem, overview of various types of attacks and to provide valuable guidance for the future research.
Keywords- DoS, DDoS, Zombie, Attacker, Master, Botnet

Citation: Abhishek Jain and Ashwani Kumar Singh (2012) Distributed Denial of Service (DDoS) Attacks- Classification and Implications. Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-136– 140.

Introduction

The Internet has seen massive growth in the number of host connect to it in the recent years and with this growth various loopholes and weaknesses in its security mechanisms have also been surfaced. Securing the Internet, as in any other field of computing, is based on the principle of confidentiality and integrity. The presence of packet sniffers, malicious routers, covert channels, and eavesdroppers in the Internet makes this extremely important problem quite challenging [1].

At Physical layer the attacker damages the physical medium like cutting the cables etc. At Data Link Layer the attacker exploits the weakness of various MAC protocols. At the Network, Transport and Application, Layer there are various loopholes in many protocols that are exploited by attackers. These loopholes are inevitable since the Internet architecture is based on the principle that the backbone network should be kept as simple as possible, pushing complexity to the edge. The protection against these types of attacks is quite difficult. Figure 2 illustrates various types of threats to such Internet (TCP/IP) protocols:

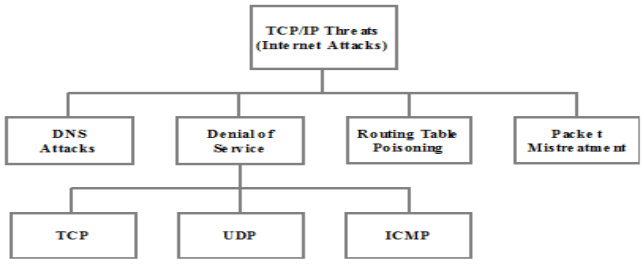

Fig. 1- Types of TCP/IP Threats

Out of these attacks denial-of-service attack is most challenging and most difficult one to prevent & trace back. A DoS attack is commonly an event in which a legitimate user or organization is deprived of certain services, such as Web, email, or network connectivity, that the user would normally expect to have [2].

Definition and Types of Dos Attacks

DoS attack is a serious problem of Internet. It is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resource [3]. A denial of service (DoS) attack is an attack that clogs up so much memory on the

target system that it can not serve it's users, or it causes the target system to crash, reboot, or otherwise deny services to legitimate users. In a DoS attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.
A Denial of Service attack usually has two forms:-

Simple Denial-of-Service attack

Is a fatal attempt by an external agent to cause a situation where the actual resource(victim undergoing attack) becomes unavailable to the actual/legitimate visitors or users. In this case there is one attacker and only one host machine is used by the hacker for the attack. Figure 2 illustrates a simple DoS attack involving only attacker machine and one target victim.

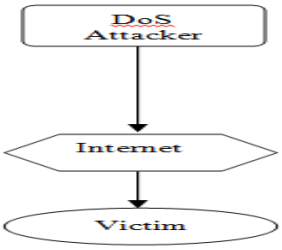

Fig. 2- Simple DoS Attack

Distributed Denial-of-Service attack: A distributed denial-of-service (DDoS) attack is one in which a many compromised systems attack a single target, thereby causing denial of service for users of the targeted system.
A distributed denial-of-service attack occurs when the attackers use several machines to launch the attack, making it more powerful. Figure 3 illustrates DDoS attack scenario

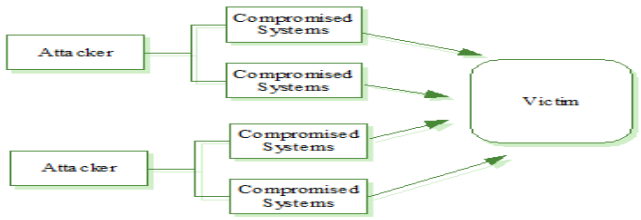

Fig. 3- Distributed DoS attack

These attacks aim at crippling applications, servers, and whole networks, disrupting legitimate users' communication. They are performed intentionally, easy to perpetrate, and very, very hard to handle. The popular form of these attacks, Distributed Denial-of-Service (DDoS) attacks, employs dozens, hundreds, or even well over 10,000 compromised computers, to perform a coordinated and widely distributed attack. It is immensely hard to defend yourself against a coordinated action by so many machines.

Implications of DDoS attacks

DoS attacks attempt to exhaust the victim's resources. These resources can be network bandwidth, computing power, or operating system data structures. To launch a DDoS attack, malicious users first build a network of computers that they will use to produce the volume of traffic needed to deny services to computer users. To create this attack network, attackers discover vulnerable sites or hosts on the network. Vulnerable hosts are usually those that are either running no antivirus software or out-of-date antivirus software, or those that have not been properly patched. Vulnerable hosts are then exploited by attackers who use their vulnerability to gain access to these hosts.
In case of hardware targeted DoS Attacks, financial losses can magnify to great extent as hosting infrastructure has to be replaced on urgent basis. This can also lead to critical data loss, if backup procedures aren't up to the mark.

There are two general forms of DoS attacks: those that crash services and those that flood services. Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System servers. A DoS attack can be perpetrated in a number of ways. The five basic types of attack effects are [4]:

- Consumption of computational resources, such as bandwidth, disk space, or processor time.
- Disruption of configuration information, such as routing information.
- Disruption of state information, such as unsolicited resetting of TCP sessions.
- Disruption of physical network components.
- Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

DDoS attackers have a significant impact over their targets. The concentrated power of even a small group of 20,000 computers can take down over 90% of Internet sites. The attacks are not limited to a specific sector but are increasingly targeting multiple, heterogeneous & unrelated types of online businesses, universities, sites and organizations.

Componets of DDoS attack

A DoS / DDoS attack can be described as an attack designed to render a computer or network incapable of providing normal services. It is considered to take place only when access to a computer or network resource is intentionally blocked or degraded as a result of malicious action taken by another user [5]. Therefore, as given by Weiler [6] it includes any of the following attempts:

-To inhibit legitimate network traffic by flooding the network with useless traffic,

-To deny access to a service by disrupting connections between two parties,

The frequency of cyber-attacks and the impact of malicious software reached epidemic proportions in 2011. This trend is continuing to accelerate into 2012 as millions of computers are compromised every month by sophisticated attackers. These infected PCs are collected and controlled in the form of "Botnets," and can be used to launch coordinated Distributed Denial of Service attacks (DDoS) and other cyber-attacks. Today's cyber-criminals regularly create new attack variants to complicate the attack strategies.
Using client server technology, the attacker is able to multiply the effectiveness of the DOS significantly by harnessing the resources of multiple ignorant collaborator computers, which serve as attack platforms.
A DDoS attack is composed of four elements [7], as illustrated in

Fig 4
-The real attacker.
-The handlers or master compromised hosts, who are capable of controlling multiple agents.
-The attack daemon agents or zombie hosts, who are responsible for generating a stream of packets towards
-The intended victim or target host.

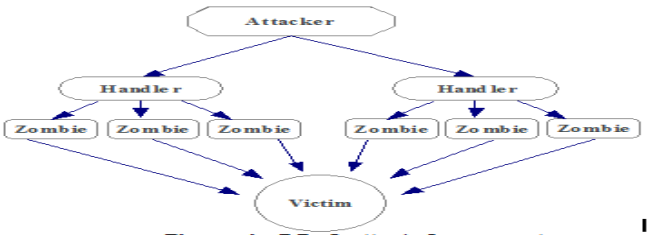

Fig. 4- DDoS attack Components

DDOS Attack Techniques

During Distributed Denial of Service attempts, attackers launch attacks using different techniques including HTTP, ICMP, SYN Floods, UDP Floods, DNS Request Floods, TCP RESET and others. The attack components are often used in combination, and range in size from a few hundred megabits per second (Mbps) to several gigabits per second (Gbps). There can be several classifications of DDoS attacks based on various criteria such as[7]
-Network Device Level include attacks that might be caused either by taking advantage of bugs in software
-OS Level: In the OS Level DOS attacks take advantage of the ways operating systems implement protocols.
-Application-based attacks
-Data Flooding: An attacker may attempt to consume the bandwidth available to a network, host or device, by sending massive quantities of data and thus causing it to process extremely large amounts of data.
Some of the polpular DDoS attacks are:

UDP Flood Attacks

UDP is a connectionless protocol that doesn't use a handshake mechanism to establish a connection. This makes it relatively easy to use it for flood attacks. In this the attacker sends a large number of forged UDP packets to random diagnostic ports on a target host. In this case mostly echo and Chargen services of UDP are exploited

TCP SYN Flood Attack

Another common example of a DoS attack is the *TCP SYN flood attack*, in which the attacker exploits the logical weakness of TCP protocol. In general a TCP connection is established by using a *three-way handshake* mechanism. When a client wants to connects to a host, it sends a SYN request to the host. The host replies with a SYN/ACK, again to synchronize. Then the client acknowledges it received the SYN/ACK packet by sending and ACK. This process is shown in figure 5.

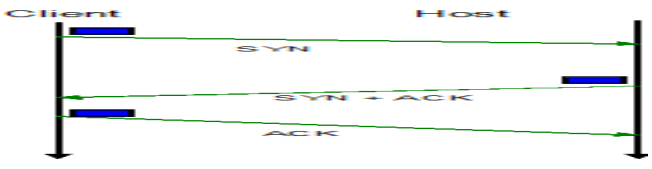

Fig 5-Normal TCP 3-way Handshake

To launch TCP SYN flood attack, the attacker creates several half-open TCP connections on the host side by sending several SYN packet with a forged IP address, upon receiving the SYN, the host allocates some memory queue and replies with a SYN/ACK but the attacker never acknowledges it. This will eventually lead to the host reaching a certain limit and may be exhausted with memory and this will prevent the host from accepting connection requests from legitimate users as well. This is shown is figure 6

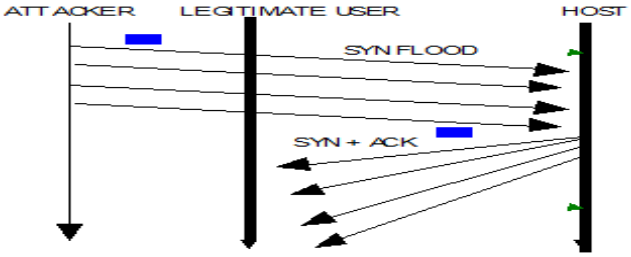

Fig. 6-TCP SYN Flood Attack

Ping of Death Attack

Another old DoS attack is the *Ping of Death*. In this attack the attacker sends a ping packet that contains more than 65,536 bytes, which is the upper limit of IP datagram size. This packet can cause the receiving machine to malfunction such as crashing and rebooting. It can lead the target system to reboot. Many older OS such as Windows versions 95 were vulnerable to the Ping of Death. Modern operating are being patched up to deal with this problem. A simple example of ping of death is :

C:/> ping 10.20.30.40 -t -l 70000

Teardrop Attack

While a IP packet is hoping from the source machine to the destination machine, it may be broken up into smaller fragments. A Teardrop attack creates a stream of IP fragments with their offset field overloaded. The destination host that tries to reassemble these overlapped fragments and eventually crashes or reboots.
For example if you are sending 20,000 bytes of data from one system A to another System B. Rather than sending the entire data in a single packet, the packet is broken down into smaller packets as given below:
-packet 1 will carry bytes 1-10000
-packet 2 will carry bytes 10001-20000.
In a teardrop attack, however, the attacker modifies the offset filed in the IP datagrams sent to the target computer and they can overlaps with each other as follows:
Packet 1 (bytes 1-15000)
Packet 2 (bytes 11001-20000)

DNS Query Attack

In this attack the attacker sends a large number of fake UDP-based DNS requests to a DNS name server using a spoofed source IP address. Then the name server, responds by sending back replies to the spoofed IP address as the victim destination.

Smurf Attacks

This is another severe type of DoS attack which is made possible because of poorly configured network devices that respond to ICMP echoes sent to broadcast addresses.
The attacker sends a large amount of ICMP echo request packets to the broadcast address of the victim IP address and uses a victim's IP address as the source IP in the ICMP request packet (Spoofed Address). When such ICMP requests reaches to all other host in the network domain they respond with a reply to the victim

address as a result the victim is overwhelmed with replies and can go down.

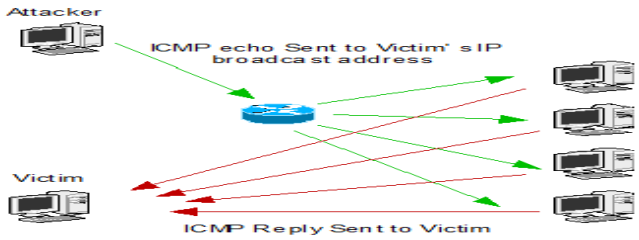

Fig 7- illustrates a typical Smurf attack scenario.

Some of the other famous documented DDoS attacks [8] [9] are as follows:

Apache

This attack is mounted against an Apache Web server where the client asks for a service by sending a request with many HTTP headers. However, when an Apache Web server receives many such requests, it cannot confront the load and it crashes.

ARP Poison

Address Resolution Protocol (ARP) Poison attacks require the attacker to have access to the victim's LAN. The attacker deludes the hosts of a specific LAN by providing them with wrong MAC addresses for hosts with already-known IP addresses. This can be achieved by the attacker through the following process:

Back Slash

This attack is launched against an apache Web server, which is flooded with requests containing a large number of front-slash (/) characters in the URL description.

CrashIIS

The victim of a CrashIIS attack is commonly a Microsoft Windows NT IIS Web server. The attacker sends the victim a malformed GET request, which can crash the Web server.

DRDoS Attacks

Unlike typical DDoS attacks, in Distributed Reflector DoS attacks the army of the attacker consists of master zombies, slave zombies, and reflectors [10]. The scenario of this type of attack is the same as that of typical DDoS attacks up to a specific stage. The attackers have control over master zombies, which, in turn, have control over slave zombies.

DDOS Attack Tools

There are different tools available to launch a DoS or DDoS attack. They differ in technique used and the in way they communicate between master and agents. some of the popular tools are :

Trinoo

Is one of the oldest DDoS attack tools used to launch a UDP flood attack on the target victim. Trinoo uses master/slave architecture and attacker controls a number of Trinoo master machines. It is a complex DDoS tool that uses "master" programs to automate the control of any number of "agent" programs which launch the actual attack.

TFN

Tribe Flood Network or TFN is a more complex and powerful tool than Trinoo. It uses command line interface to communicate between attacker and control master program. Just like *trinoo* it uses a master program to communicate with attack agents located across multiple networks. *TFN* launches coordinated Denial of Service Attacks that are especially difficult to counter as it can generate multiple types of attacks and it can generate packets with spoofed source IP addresses.

TFN2K

Is a more advance form of TFN. It can launch different types of attacks randomly at once such as TCP SYN, UDP Flood, ICMP Flood , Smurf etc. The main advantage of TFN2K is that the communication between the master and agents is encrypted.

Stacheldraht

Stacheldraht combines the features of TFN and Trinoo but adds encryption layer between daemons. Trinoo uses UDP for communication between handlers and agents, TFN uses ICMP for communication between the handler and agents, and Stacheldraht uses TCP and ICMP. Another big difference is the use of encryption. Control of a

Shaft

Shaft is relatively similar to Trinoo, except that the port number used are different than Trinoo. Shaft is a packet flooding attack. Shaft can implement UDP, ICMP, and TCP flooding attack.

Trinity

This tool uses TCP port 6667 and also has a backdoor component that listens on TCP port 33270.

Tables 1 illustrate some common DDoS tools and types of attack they support:

Table 1- DDoS Tools and Attack Methods

Trinoo	UDP
TFN	UDP, ICMP, TCP
Stacheldraht	UDP, ICMP, TCP
TFN2K	UDP, ICMP, TCP
Shaft	UDP, ICMP, TCP
Trinity	UDP, TCP

DDOS Defence Principles

Regardless of the continuous effort and resources spent securing against intrusion, Internet faces a consistent and real threat from DoS attacks because of two fundamental characteristics of the Internet.

1. The Internet is comprised of limited and consumable resources
2. Internet security is highly interdependent

Currently there are many challenges development effective DDoS defense mechanisms. These challenges include [11]

(a) Large number of ignorant participants
(b) No common characteristics of DDoS streams
(c) Use of legitimate traffic models by attackers
(d) No administrative domain cooperation
(e) Use of automated tools
(f) Hidden identity of participants
(g)Absence of standardized evaluation and testing approaches.

Thus, the following five principles are recommended [12] to build an effective solution:

1. DDoS is a distributed attack and because of high volume and rate of attack packets, distributed instead of centralized defense is the first principle of DDoS defense.
2. It has a High Normal Packet Survival Ratio (NPSR), hence, less collateral damage is the prime requirement for a DDoS defense.
3. A DDoS defense method should provide secure communication

for control messages in terms of confidentiality, authentication of sources, integrity, and freshness of exchanged messages between defense nodes.
4. A partially and incrementally deployable defense model that does not need centralized control will be successful.
5. A defense system must take into account future compatibility issues such as interfacing with other systems and negotiating different defense policies.

DDOS Defence Techniques

There are various safety precautions that would make the host and the network and more secure. These measures include:

Filtering Routers

Filtering all packets entering and leaving the network protects the network from attacks conducted from neighboring networks, and prevents the network itself from being an unaware attacker [13].

Disabling IP Broadcasts By disabling IP broadcasts, host computers can no longer be used as amplifiers in ICMP Flood and Smurf attacks.

Applying Security Patches

To guard against denial of service attacks, host computers must be updated with the latest security patches and techniques.

Disabling Unused Services If UDP echo or chargen services are not required, disabling them will help to defend against the attack.

Performing Intrusion Detection

By performing intrusion detection, a host computer and network are guarded against being a source for an attack [15].

Conclusion

DDoS attacks are the biggest threat to Internet services and with the growth of Internet the problem is also growing exponentially. In this survey paper we discussed the problem of DDoS attack and current defense mechanisms.. Currently the defense mechanisms are mainly passive in nature and there is a need to develop some novel techniques to handle them. Also, there is no sufficient security patches on all hosts in the Internet and there are unrelenting security holes in Internet Infrastructure. Finally following are the concluding remarks:

- Current defense mechanisms are far from adequate.
- One promising direction is to develop a global infrastructure.
- Deployment and design considerations should be worked upon.

Acknowledgement

The author sincerely acknowledges the guidance, support and encouragement given by Prof. B. B. Gupta, Dept of Computer Science, Graphic Era University. I also thank my other colleagues for their help and cooperation.

References

[1] Pfleeger C.P. (1996) *Prentice Hall.*
[2] Gupta B.B., Joshi R.C. and Misra Manoj (2009) *Information Security Journal: A Global Perspective,* 18: 5, 224 — 247.
[3] Computer Emergency Response Team (2001) *http:// www.cert.org.*
[4] *http://en.wikipedia.org/wiki/Denial-of-service_attack*
[5] Douligeris C., Mitrokotsa A. (2004) *Computer Networks,* Volume 44, Issue 5, pp. 643-666.
[6] Weiler N. (2002) *Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, *Pittsburgh, USA,* pp. 109-114.
[7] Douligeris A., Mitrokotsa (2003) 3*rd IEEE International Symposium on Signal Processing and Information Technology* 03), Darmstadt, Germany, pp. 190-193.
[8] *www.ll.mit.edu/IST/ideval/docs/1999/attackDB.html.*
[9] Yanet Manzano (2003) *http://www.acm.org/crossroads/xrds10-1/tracingDOS.html.*
[10] Steve Gibson (2002) *Distributed Reflection Denial of Service Description and Analysis of a Potent, Increasingly Prevalent, and Worrisome Internet Attack*.
[11] Kumar K., Joshi R.C. and Singh K. (2006) *IRISS*, *IIT Madras.*
[12] Robinson M., Mirkovic J., Schnaider M., Michel S. and Reiher, P (2003) *SIGCOMM*.
[13] Ferguson P. and Senie D. (1998) *Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing*.
[14] Cisco Systems (1999) *http://www.cisco.com/*.
[15] Ptacek T.H. and Newsham T.N. (1998) *Secure Networks, Inc*.