Host-based Intrusion Detection against Distributed Denial of Service Attacks

Harmeet Kaur
Dept. of CSE, Lovely Professional University, Phagwara, India
E-mail: harmeet_kaur11@yahoo.com

Abstract

One of the greatest threats that network security faces nowadays is Distributed Denial of Service attacks. A newer version of the Denial of Service attack, also called Distributed Denial of Service attack or DDoS. In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. An attacker may attempt to: "flood" a network and thus reduce a legitimate user's bandwidth, prevent access to a service, or disrupt service to a specific system or a user. In this paper describe methods and techniques used in denial of service attacks. In this study, simulate a distributed denial of service attack using ns-2 network simulator. The detection is host based and in this simulation we have attacker and victim computer and attacker is distributed means attacker use other different computers to impose the attack on victim. This work on intrusion detection cannot prevent or defend against DDoS, it is applicable to help the security administrators detect a DDoS attack and take actions as soon as possible to avoid greater loss.

Key words. Distributed Denial of Service, Host -based Intrusion Detection , Flood attack, Simulation

1 Introduction

Multiple-source DoS attacks are called distributed denial-of-service (DDoS) attacks. DDoS attacks can sometimes employ up to 100,000 compromised computers to perform a coordinated and widely distributed attack. In most attacks, the source address is faked . This means that the attacker uses other people's computers to run the attack. The users who are used in such attack normally do not know that they have been used in an attack. Distributed denial of service(DDoS) [8] attacks make the resources of host occupied largely via sending many malicious packets, which results in the failure of normal network services. DDoS attack the target host through constructing a lot of illegal packets. Distributed Denial of Service (DDoS) attacks launched against major Internet sites in February 2000 [6] brought a stark reality to the Internet E-Commerce community as small hosts attacked large allegedly well-protected systems. In this paper use a network simulator to study distributed denial of service attacks. This simulation shows how the problem of denying bandwidth to legitimate users during the distributed denial of service attack.

2. Components of of a distributed denial of service attack

A distributed denial of service attack is composed of four elements, as shown in Figure 1 [7].

- First, it involves a victim, i.e., the target host that has been chosen to receive the brunt of the attack.
- Second, it involves the presence of the attack daemon agents. These are

agent programs that actually conduct the attack on the target victim. Attack daemons are usually deployed in host computers. These daemons affect both the target and the host computers. The task of deploying these attack daemons requires the attacker to gain access and infiltrate the host computers.

- The third component of a distributed denial of service attack is the control master program. Its task is to coordinate the attack. Finally, there is the real attacker, the mastermind behind the attack. By using a control master program, the real attacker can stay behind the scenes of the attack.

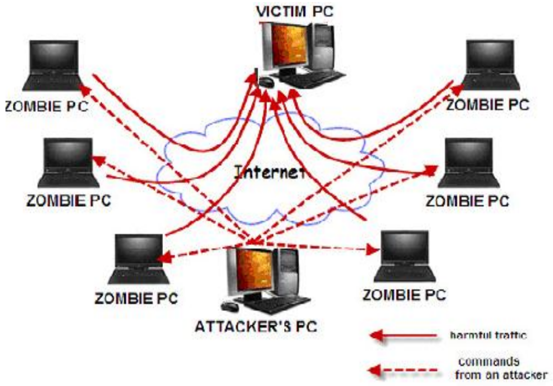

Figure 1 : DdoS components

A DDoS attack is a distributed form of denial-of-service attacks. DoS attacks consume the resources of a remote host or network by sending large numbers of IP packets over a short time period. While a single host can cause significant damage by sending packets at its maximum rate, attackers can mount more powerful attacks by leveraging the resources of multiple hosts. In a typical DDoS attack, an attacker first intrudes into as many hosts as possible and installs two kinds of ‘zombie’ program: control program (master zombie) and flooding program (slave zombie).

3. Impact of a DDoS attack

The impact of a DDoS attack can be classified into the following categories:

Destructive: The attack prevents a device from performing its legal functions. This involves power interruption or destruction of configuration information.

Resource consumption: The attack degrades the ability of a resource to function. This is achieved with the over usage of resources.

Bandwidth consumption: This attack overwhelms the bandwidth capacity of a network. This is achieved by sending bogus requests to victim sewers. Thus clogging the network with traffic.

4. Classification Of Attacks

DDoS attack can be flooding attack or vulnerability attack [3], [5]. Flooding attack eats up the victim resources by flooding the large volume of packets. Vulnerability attacks use the expected behavior of protocols such as TCP and HTTP to the attacker’s advantage.There are varieties of DDoS attacks as classified in [3], [4]. However, the most common form of DDoS attacks is a packet-flooding attack, in which a large number of seemingly legitimate TCP, User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) packets are directed to a specific destination.

4.1 UDP Flood : A stream of UDP packets are sent to the victim IP address.As it is specified, a server receiving a UDP packet on a closed port sends back an ICMP Port Unreachable packet to the source[1]. The data part of the ICMP packet is filled with at least the first 64 bytes of the original UDP packet. As no limit or quota is specified as a standard, it is then possible to send huge amount of packets on closed ports. At very high load, operations necessary to generate ICMP error packets consume a lot of CPU, eventually leading to CPU resource exhaustion.

4.2 Smurf attack: A bandwidth attack, such as a "Smurf" attack, targets a feature in the IP specification known as "direct broadcast addressing" to quickly flood the target host or network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings)[5]. The hacker sets the destination IP address of each packet to the broadcast address of the network, causing the router to broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "amplifier" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

4.3 SYN Flood attack: SYN Flood attack is also known as the Transmission Control Protocol (TCP) SYN attack,DDoS attacks use TCP [2]. The TCP SYN flooding is the most commonly-used attack. It consists of a stream of spoofed TCP SYN packets directed to a listening TCP port of the victim. The SYN flooding attacks exploit the TCP's three-way hand-shake mechanism and its limitation in maintaining half-open connections. When a server receives a SYN request, it returns a SYN/ACK packet to the client. Until the SYN/ACK packet

is acknowledged by the client, the connection remains in half- open state for a period of up to the TCP connection timeout,which is typically set to 75 seconds. The server has built in its system memory a backlog queue to maintain all half-open connections. Since this backlog queue is of finite size, once the backlog queue limit is reached, all connection requests will be dropped.

5. How DDoS Attacks are executed

DoS Attacks are usually executed by flooding the target servers with unsolicited data packets in unprecedented manner. This may be done by misconfiguring network routers or by performing smurf attack on the victim servers. This results in 'Capacity Overflow', followed by Max Out of system resources, which makes the target service unavailable, either temporarily or permanently(In case of hardware targeted DoS attack) to the intended users.

In case of DDoS attack, the origin of unsolicited data packets (for the purpose of flooding the bandwidth/resource of the victim servers) are distributed over a large network(or internet). The overall mechanism of DDoS Attack involves a huge quantity of compromised network nodes (computers connected to internet), governed by agent handlers, which are further controlled centrally by the actual attacker. The massive number of compromised computers on the internet are then unknowingly governed by the source attacker to demand access to the targeted victim within a minimal time span, which further causes saturation of limited system resources and results in eventual shutdown of the targeted service.

6. Simulation and results

The simulation tool is ns2.The network structure for attacking simulation is indicated in figure 2.The node n0 represent the legitimate user and node n1,n2,n5 stands for attacker,n3 for the router and n4 for the target.this simulat a simplified version of distributed denial of service attack on a single targeted router. The simulation is done by the attack using UDP packets. The goal of this paper is to measure the throughput provided to the legitimate users and to the attackers when using the drop-tail queuing method.

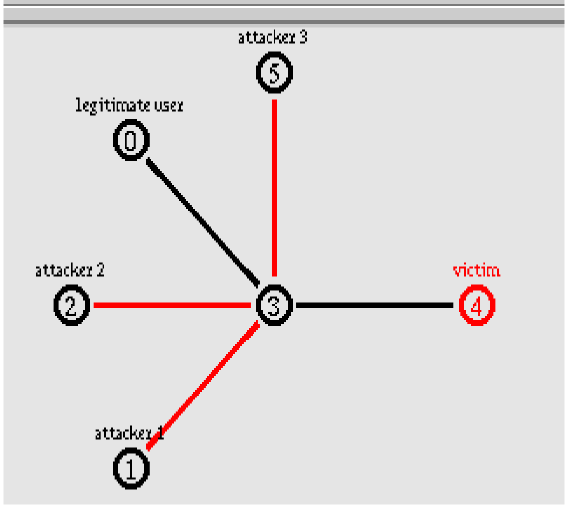

Figure2 :Attacking structure for simulation

In this simulation scenarios, here is a single target router with a 1 Mbps bandwidth and other links have 1Mbps bandwidth ,with delay of 100msThe legitimte user send UDP packets of size 500 bytes at the rate of .1 Mbps. But the attackers sending TCP and UDP packets of size 500 bytes at the rates of 0.3 to 1.0 Mbps. All sources generated constant bit rate traffic. *DropTail* is a queuing algorithm based on a first-comefirst- serve discipline.

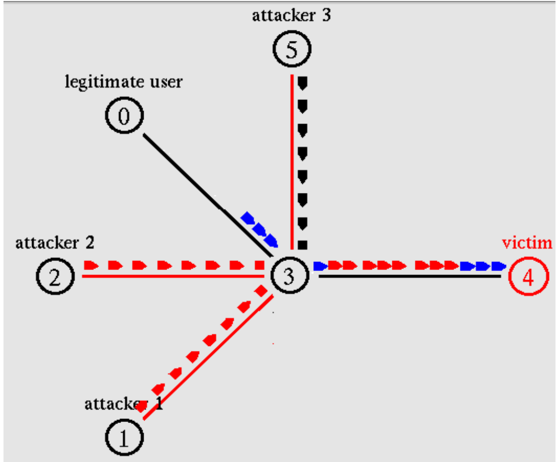

Figure3: Before packets drop

Figure 3 shows how the packets are sent to victim computer by legitimate user and other attackers. The packets of user is received by victim but During flooding attack the attackers congest the victim's access router by flooding packets towards victim. This results in the consequence that the legitimate clients are denied of the service due to limited bottleneck bandwidth see figure 4.

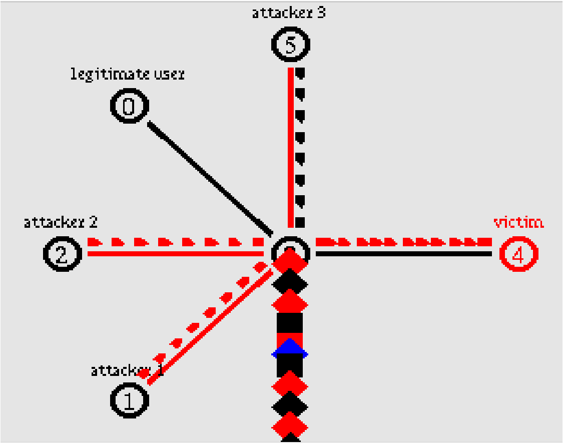

Figure4 :After Packets drop during DDoS attack

In the DropTail queuing algorithm, we have three attackers that overload the target router. The legitimate user has 0.1Mbps, . Since the target router has a buffer size of 1Mbps, and the input links have 1.3 Mbps bandwidth,overloading the buffer in the router only requires three attackers and packet loss in the router is to be expected.

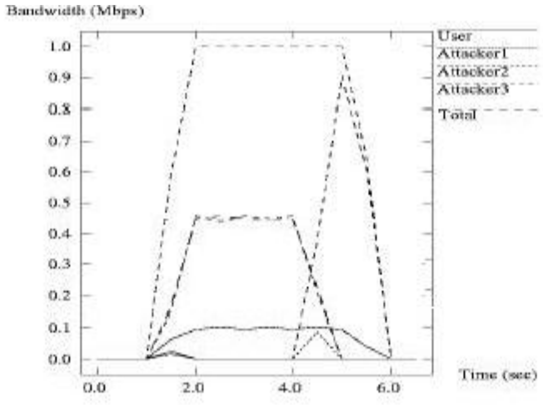

Figure5:Simulation results using DropTail queuing algorithm

In the figure one legitimate user, Attacker 1, Attacker 2, attacker 3 the total bandwidth. The legitimate user’s bandwidth was reduced to zero once the attack executed by the three attack daemons was fully engaged. As shown in Figure5, the user's bandwidth (bottom curve) falls to zero at approximately 2.5 sec after the beginning of the attack.Once the attack is fully engaged, the legitimate user (bottom curve) is left with little or no bandwidth.

7. Conclusions

In this paper, a host-based intrusion detection technique to detect against distributed denial of service is proposed and analyzed. First analyze the different DDoS attacks and how these attacks are executed .Denial-of-service attacks occur almost every day, and the frequency and the volume of these attacks are increasing day by day. The network simulation tools are used to detect the distributed denial of service attacks .In this paper the simulation shows when the attackers execute attack then the user's bandwidth is used by attackers and provided no bandwidth to the legitimate user during the attack.. In summary, the simulation results indicated that implementing drop-tail queuing algorithm in network router may provide the desired solution in protecting users in cases of distributed denial of service attacks.

References

[1] T. Simcock, “Distributed Denial of Service Attacks: Threats, Motivations & Management”, GIAC practical repository, SANS Institute, Nov. 2002.

[2] D. Moore, G. Voelker and S. Savage, “Inferring Internet Denial of Service Activity”, Proceedings of USENIX Security Symposium’2001, August 2001.

[3] J. Mirkovic, and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” Computer Journal of ACM SIGCOMM, vol. 34, no. 2, pp. 39-53, Apr. 2004.

[4] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state of the art," Computer Journal of
Networks, vol. 44, no. 5, pp. 643-666, Apr.2004

[5] T. Peng, C. Leckie, and K. Ramamohanarao, “Survey of network based defense mechanisms countering the DoS and DdoS problems,” Computer Journal of ACM Computing Surveys, vol. 39, no. 1, pp. 123-128, Apr. 2007.

[6] Consensus Roadmap for Defeating Distributed Denial of Service Attacks. Global Incident Analysis Center ---- Special Notice. 1999-2000 SANS Institute, http://www.sans.org/ddos_roadmap.htm.

[7] S. Bellovin, “Distributed denial of service attacks,” Feb. 2000, http://www.research.att.com/~smb/talks.

Harmeet Kaur has completed her M.Sc in computer science and pursuing her M.Tech in CSE from LPU,Phagwara,Punjab,India.

E-mail: harmeet_kaur11@yahoo.com