Frequent Denial of Service Attacks

Aditya Vutukuri
Computer Science Department
University of Auckland
E-mail:avut001@ec.auckland.ac.nz

Abstract

Denial of Service is a well known term in network security world as it is considered as one of the most dreaded network based attacks which can leave our system unusable or unreachable. It can happen to any one sitting on the network unprotected .So, a good understanding of the frequent attacks is very important for the common users on a network as it can provides minimal protection to the users from these attacks. In this paper, I have discussed the simple structure of denial of Service attacks and its effects on the victim. This paper also discusses some of the most common forms of these attacks and how they happen. What I am discussing here is clear understanding of DoS (Denial of Service) attacks and the possible prevention as it is well said by our elders "Prevention is Better than Cure".

1. Introduction

As we go on relying more on networks for rapid transfer of information and faster ways of communication, it becomes important for us to safe guard ourselves from various hazards caused by various other malicious users on the network. Whenever a user connects his system to the network his basic concern is to keep his system safe from malicious attacks .And DoS is one of the attacks of this category that is now bothering the whole Internet community these days .So, it is important that a common user knows what DoS can do. When a user is under DoS attack, his system or his recourses become unreachable to himself and he may even loose the total control of his system. This may happen to any

one on the network and this paper gives a reader the basic understanding for most frequent of the DoS attacks.

In this paper as we go on, we will be discussing the working of general DoS attacks, the reasons behind the attack and the effects of these attacks on the users. We will also be seeing the most frequently used DoS attacks like Buffer over flow attacks which are attained by sending more and more data to a device than it can actually handle which in turn jams the device and in turn interrupts the device's normal functioning and thus causing the problem to the user of the device. We will also be discussing other TCP/IP based DoS attacks like SYN[4] attacks which uses the TCP connection request SYN[4] to lash up as many resources as possible of a target computer. We will also be discussing other frequent DoS attacks which use TCP/IP for configuring the attacks like LAND attack and Teardrop attack; we will be discussing them in the next couple of pages. We will also discuss how an attacker uses ICMP[1] for making up the attack. When doing this attack the attacker makes use of the most commonly used command "ping "to launch the attack on the target system which we will discuss in much detail later.

The major aim of this paper is to discuss and understand various most frequent DoS attacks and their possible prevention. The rest of this paper is organized as follows. First, the section 2, we discuss the general structure of DoS attack and the various roles involved in it. Here we will also quickly discuss the reasons behind doing the DoS attack .In section 3 will be discussing the most frequent DoS attacks like SYN[4] attack, LAND, Buffer overflow, Teardrop and Smurf attack. Finally in section 4 we will include the conclusion of the paper**.**

2. Structure of Denial of Service attack

The target of most DoS attacks is to render the target machine on the network inaccessible to the legitimate users. If we see the structure of the Denial of Service attack we can divide it into 3 roles:

1) Malicious user (Attacker)
2) Network or System (Medium)
3) User or Users (Victim)

Here, we shall discuss each of the 3 roles very briefly.

2.1 Malicious user (Attacker):

They are the people who want to affect the network for many reasons. They have more and more accessibility to networks as networks are growing very rapidly. They compromise the network by getting hold of some key security holes missed by the network administrator of that network to launch the possible attack through it. There may be many probable reasons behind launching the attack like:

1) To gain access
2) Economical reasons
3) Political reasons
4) Revenge
5) Sub-cultural status etc.

2.2 Network or System (Medium):

The most common targets of the attack are various networks, large or small. The attacker uses these networks as a medium to launch their attacks. The attack may even be directed towards an individual user on the network. After compromising some security holes in the network.

2.3 User or Users (Victim):

The Victim is the person who is connected in the effected network and is not able to receive the services which he used to receive. There may be single or multiple victims. In case of a single victim the user‘s system may be unattainable or unreachable. It may be of many sorts like the system getting crashed or something like that.

The figure on the next page gives a better understanding of the working of DoS attacks. The figure 1 shows how the attacker affects multiple users connected on a network .The figure 2 shows how the attacker affects a single user connected on a network. In this case all the remaining connected users will be unaffected and they may be using the service very normally. This attack may be directed to more than two users also

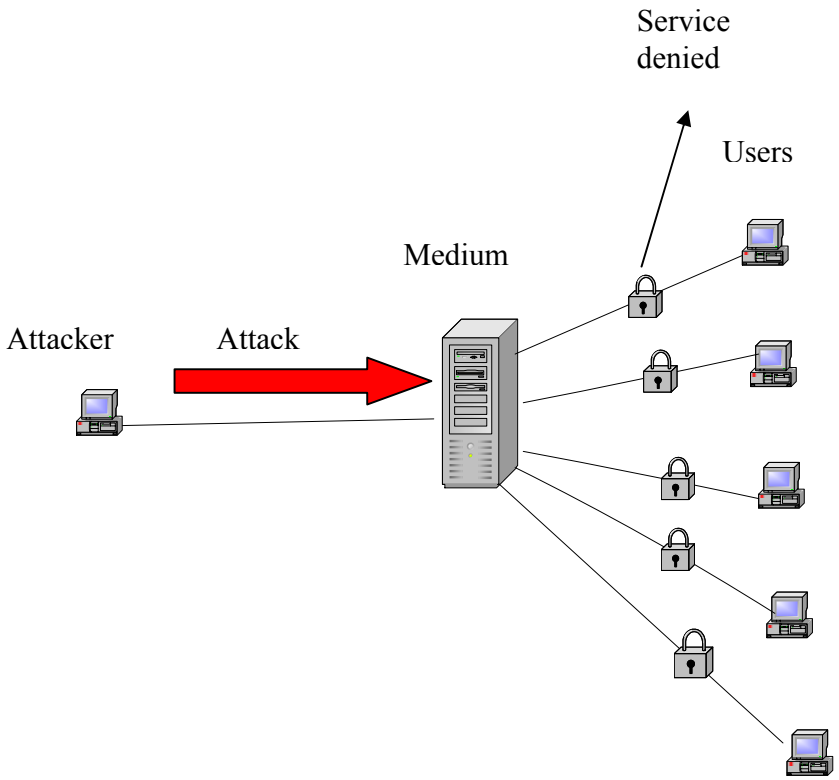

Figure 1

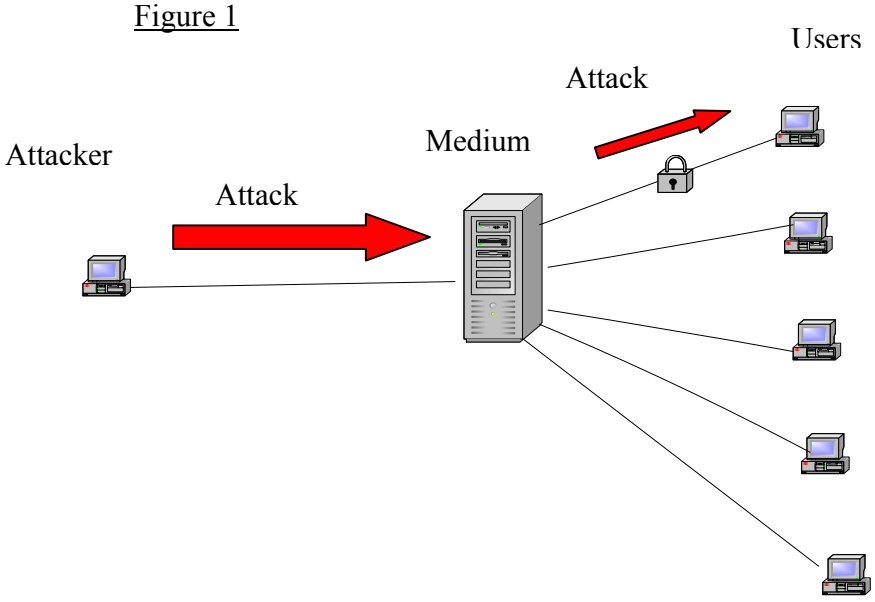

Figure 2

In general various attacks on network fall into any one of the following form:

1) Mail bombing to individuals, lists or domains.
2) Passing the server bogus requests.
3) Typing up CPU cycles, memory or other resources.
4) Misconfiguring the router (occurs accidentally).

Computer

3. Frequent Denial of Service attacks

Although the DoS attacks are becoming a serious threat day by day, the basic intent of the attacks remains the same. As this threat grows on increasing, it becomes important on our part to understand the frequent attacks and how they are actually done. I will be discussing these attacks in this section.

Almost all attacks that directly target the host machines have been overcome by the patches in the operating systems. The attacks that use some features of TCP/IP protocol were quite difficult to overcome. TCP/IP is a protocol, the use which cannot be avoided when we are working on a network. And when it causes the major problems, then it is really a hard part to solve. The most common attacks because of this TCP/IP is discusses hereon.

3.1. Smurf attack

In Smurf attack the attacker uses the most common ICMP[1] protocol of IP to launch the attack on the target network. Here the attacker uses the ICMP[1] ping command to perform the attack. ICMP[1] is one of the most important protocols in TCP/IP and it is used for DNS resolution, routing, connectivity and many other things. The ICMP[1] protocol uses different messages to identify the purpose of the packet.

Let us see a simple message used in ICMP[1] and how it works:

1) First, an ICMP ECHO request packet is sent to a system.

2) Then the receiving machine will return with ICMP ECHO reply packet.

In this smurf attack the attacker sends an ECHO request message directed to broadcast addresses. While doing so the attacker gives the source address as the source address of the machine he intends to attack. When this request is received by other machines on the network, all of them respond with ECHO reply to the target machine. As the number of requests are very high and cannot be managed by the amount of buffer allocated by the target machine. The machine experiences DoS and thus been attacked. During the process of this attack, the attacker may also affect other users on the network. The good description of Smurf attack can be seen at[3]. The figure 2 on the next page will explain the attack in much detail.

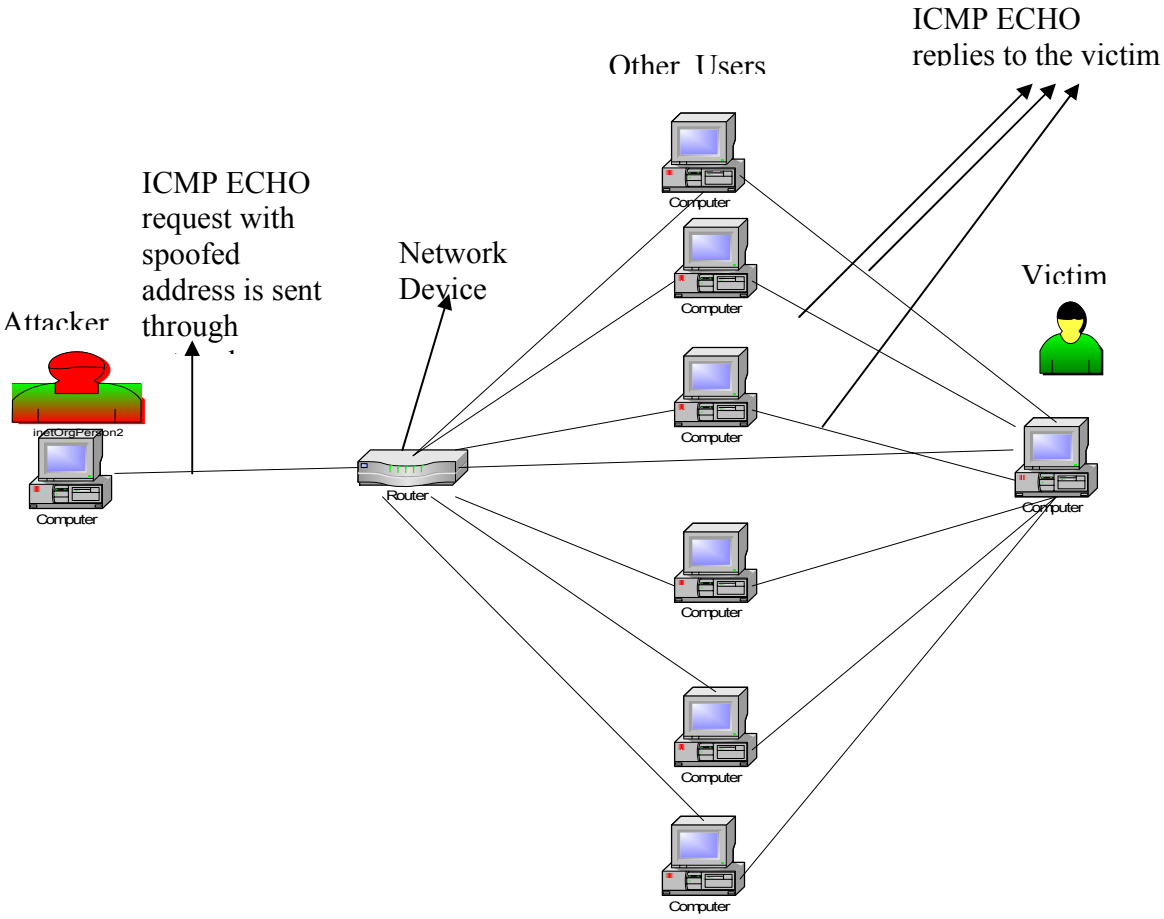

Figure 3

Possible Preventions of the attack:

It is very difficult to stop smurf attacks as the attacker is taking the advantage of one of the features of ICMP[1] protocol.

1) One way to stop it is to use Operating Systems that are aware of flooding with ICMP[1], and will begin to drop the packets or block the connection.
2) "Disable IP-directed broadcasts at your router" [6].

These are just some possible simple preventions and it may not be necessary that they are the best safety measures because when you are connected on a network there is nothing called perfect security system.

3.2 SYN attack

As I told before TCP/IP is something which cannot be avoided when on the network and hackers use this as a weakness for launching their dreadful attacks. In

SYN[4] attack the hacker uses the connection requests in TCP to launch their intended attack. They use the SYN command here. The attacker sends many fake TCP connection requests (SYN) to target machine and the target machine as usual accepts all of them. Here again the attacker spoofs his source address to escape simple filtering. When target machine receives the request, it as usually allocates the requested resource for the request and sends the SYN acknowledgement. The requests are stored in the target's request table and are processed one after the other and never end as the number of requests is very high. This further avoids it from recognizing the legitimate requests of the later users. Thus the attack is successfully launched. One can easily verify the system is under attack [5] using a simple command on your dos (Disk Operating System here) prompt.

netstat –n –p tcp

and you can see the following test:

```
  Protocol  Local Address          Foreign Address        State

    TCP    127.0.0.1:1030         127.0.0.1:1032         ESTABLISHED

    TCP    127.0.0.1:1032         127.0.0.1:1030         ESTABLISHED

    TCP    10.57.8.190:21         10.57.14.154:1256      SYN_RECEIVED

    TCP    10.57.8.190:21         10.57.14.154:1257      SYN_RECEIVED

    TCP    10.57.8.190:21         10.57.14.154:1258      SYN_RECEIVED

    TCP    10.57.8.190:21         10.57.14.154:1259      SYN_RECEIVED

    TCP    10.57.8.190:21         10.57.14.154:1260      SYN_RECEIVED

    TCP    10.57.8.190:21         10.57.14.154:1261      SYN_RECEIVED

    TCP    10.57.8.190:21         10.57.14.154:1262      SYN_RECEIVED

    TCP    10.57.8.190:21         10.57.14.154:1263      SYN_RECEIVED

    TCP    10.57.8.190:21         10.57.14.154:1264      SYN_RECEIVED

    TCP    10.57.8.190:21         10.57.14.154:1265      SYN_RECEIVED

    TCP    10.57.8.190:21         10.57.14.154:1266      SYN_RECEIVED

    TCP    10.57.8.190:4801       10.57.14.221:139       TIME_WAIT
```

Figure 4[5]

In the above figure you can easily find out from the stack that you system is under attack. So you can now take the action.

Probable prevention techniques:

1) One can prevent this by increasing the buffer size to hold more requests. But here I felt we are really compromising with the security, But we must make some compromises for security sometimes.

2) We can also prevent some attacks by adding patches to the operating system which can detect and remove such SYN requests which are running for more than required predefined period. This has already been implemented in one of the Cisco routers. This defense is called TCP intercept [7].

3.3 LAND attack:

This is one more TCP/IP specific attack. Here the attacker again uses the SYN to attack the target system. Here the attacker uses a spoofed packet with SYN flag .The attacker spoofs the packet to have same destination and source address and this in turn generates the attack. In a simple way to say, the hacker makes the target system respond to itself and binding its resources. This attack in some cases may even crash the target system in case of few operating systems.

Probable prevention techniques:

1) There is no complete cure of this attack but it can certainly be prevented if the network administrators of the various networks take necessary care by filtering [2] all outgoing packets from the network which have different source address different from the internal network address.
2) Various vendors are providing different patches for their respective operating system [6].

3.4 Teardrop attack:

This attack again uses the vulnerability in a TCP/IP protocol. Here the attacker exploits fragmentation part of IP. The attacker attacks by sending pairs of identical

fragments of the packet which are reassembled when the data packet is received at the receiver's end. These identical fragments cause a considerable confusion in the UDP packet which can create problems like system crash down.

3.6 Buffer Overflow attack:

This is most regular attack that can be performed on a vulnerable system. It uses the resource space allocated (or buffer) for various purposes to launch the attack. Normally when we send a request to a system or a personal computer, the network interface card process them one at a time and during this time all the remaining requests are stored in the Buffer until their turn comes up. This is how most of the software and hardware devices work.

Now, when an attacker wants to perform the attack on a target, He sends more and more requests or data to a system. And when this amount of data or requests exceeds the limit of the data the target device can handle, the target experiences DoS.

This attack can be performed in many ways, but the most frequent attacks use

1) Mail bombing :here the attacker uses 256 character file names, as attachments to be sent to the target.
2) Oversized ping messages in ICMP.

Probable prevention techniques:

One way to prevent this sort of attack is by using attack sensing devices which disconnect the connection when the target is receiving more pings than it is designed to handle. There are patches available to counter mail bomb attack also; the only thing to do is the administrator must upgrade these patches from the respective venders [6].

4. Conclusion:

Network Security has always been a major area of research. The simple reason for this is, because of this network many people in various parts of the world are able to communicate with each other and transfer their important data with less effort in less time. DoS has always been an attack of discussion because of its terrible effect on the network and its user whenever it has struck.

In this paper I have discussed how these DoS attacks work, what they can do to the users and what are the possible preventions available. I have not proposed any possible solutions for the various attacks discussed in this paper. I have discussed them because a proper understanding of various DoS attack can help in effectively defending these attacks. I believe a common user must know these attacks to provide the basic security to his system and his resources.

Reference:

[1] A.Conta and S.Deering, Internet control message protocol (ICMPv6) for the Internet Protocol version 6(IPv6) Specification, RFC2463, Internet Engineering Task Force, Dec 1998.

[2] P.Ferguson, D.Senie, Network Ingress Filtering: Defeating Denial of Service Attacks which employs IP Source Address Spoofing, RFC2267, The Internet society, Jan 1998.

[3] Craig A.Hugen, The Latest in Denial of Service Attacks:"Smurfing" description and information to minimize effects, Tue Feb 8 17:47:36 PST 2000.Available at:http://governmentsecurity.org/articles/THELATESTINDENIALOFSERVICEATTACKSSMURFING.php

[4] C.Schuba, I.Krsul, M.Kuhn, G.Spafford, A.Sundram,and D.Zomboni.Analysis of Denial of Service attack on TCP, In proceeding of 1997 IEEE symposium on Security and Privacy, Page 208-223,IEEE Computer Society Press, May 1997.

[5] Microsoft: Available at:http://support.microsoft.com/default.aspx?scid=KB;EN-S;Q142641&ID=KB;EN-US;Q142641

[6] CERT: Available at: http://www.cert.org/advisories/CA-1998-01.html, http://www.cert.org/advisories/CA-1997-28.html, http://www.cert.org/advisories/CA-2003-09.html

[7] CISCO: Available at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/intercpt.htm