
DOS Attacked!!! By Ankit Fadia Ankit@bol.net.in

Date Released: 25th June 2001

DOS Attacks or Denial Of Services Attack have become very common amongst Hackers who use them as a path to fame and respect in the underground groups of the Internet. 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.

DOS Attacks are of the following different types-:

1. Those that exploit vulnerabilities in the TCP/IP protocols suite.
2. Those that exploit vulnerabilities in the Ipv4 implementation.
3 There are also some brute force attacks, which try to use up all resources of the target system and make the services unusable.

Before I go on with DOS attacks, let me explain some vulnerabilities in TCP/IP itself. Some common vulnerabilities are Ping of Death, Teardrop, SYN attacks and Land Attacks.

Ping of Death

This vulnerability is quite well known and was earlier commonly used to hang remote systems (or even force them to reboot) so that no users can use its services. This exploit no longer works, as almost all system administrators would have upgraded their systems making them safe from such attacks.

In this attack, the target system is pinged with a data packet that exceeds the maximum bytes allowed by TCP/IP, which is 65 536. This would have almost always caused the remote system to hang, reboot or crash. This DOS attack could be carried out even through the command line, in the following manner:

The following Ping command creates a giant datagram of the size 65540 for Ping. It might hang the victim's computer:

C:\windows>ping -l 65540

Teardrop

The Teardrop attack exploits the vulnerability present in the reassembling of data packets. Whenever data is being sent over the Internet, it is broken down into smaller fragments at the source system and put together at the destination system. Say you need to send 4000 bytes of data from one system to the other, then not all of the 4000 bytes is sent at one go. This entire chunk of data is first broken down into smaller parts and divided into a number of

packets, with each packet carrying a specified range of data. For Example, say 4000 bytes is divided into 3 packets, then:

The first Packet will carry data from 1 byte to 1500 bytes
The second Packet will carry data from 1501 bytes to 3000 bytes
The third packet will carry data from 3001 bytes to 4000 bytes

These packets have an OFFSET field in their TCP header part. This Offset field specifies from which byte to which byte does that particular data packet carries data or the range of data that it is carrying. This along with the sequence numbers helps the destination system to reassemble the data packets in the correct order. Now in this attack, a series of data packets are sent to the target system with overlapping Offset field values. As a result, the target system is not able to reassemble the packets and is forced to crash, hang or reboot.

Say for example, consider the following scenario-: (Note: _ _ _ = 1 Data Packet)

Normally a system receives data packets in the following form, with no overlapping Offset values.

_ _ _ (1 to 1500 bytes) _ _ _ (1501 to 3000 bytes) _ _ _ (3001 to 4500 bytes)

Now in a Teardrop attack, the data packets are sent to the target computer in the following format:

_ _ _ (1 to 1500 bytes) _ _ _ (1500 to 3000 bytes) _ _ _ (1001 to 3600 bytes)

When the target system receives something like the above, it simply cannot handle it and will crash or hang or reboot.

SYN Attack

The SYN attack exploits TCP/IP's three-way handshake. Thus in order to understand as to how SYN Attacks work, you need to first know how TCP/IP establishes a connection between two systems. Whenever a client wants to establish a connection with a host, then three steps take place. These three steps are referred to as the three-way handshake.

In a normal three way handshake, what happens is that, the client sends a SYN packet to the host, the host replies to this packet with a SYN ACK packet. Then the client responds with a ACK (Acknowledgement) packet. This will be clearer after the following depiction of these steps-:

1. Client --------SYN Packet---------- à Host

In the first step the client sends a SYN packet to the host, with whom it wants to establish a three-way connection. The SYN packet requests the remote system for a connection. It also contains the Initial Sequence Number or ISN of the client, which is needed by the host to put back the fragmented data in the correct sequence.

2. Host ----------SYN/ACK Packet---------- à Client

In the second step, the host replies to the client with a SYN/ACK packet. This packet acknowledges the SYN packet sent by the client and sends the client its own ISN.

3. Client ----------ACK---------- à Host

In the last step the client acknowledges the SYN/ACK packet sent by the host by replying with a ACK packet.

These three steps together are known as the 3-way handshake and only when they are completed is a complete TCP/ IP connection established.

In a SYN attack, several SYN packets are sent to the server but all these SYN packets have a bad source IP Address. When the target system receives these SYN Packets with Bad IP Addresses, it tries to respond to each one of them with a SYN ACK packet. Now the target system waits for an ACK message to come from the bad IP address. However, as the bad IP does not actually exist, the target system never actually receives the ACK packet. It thus queues up all these requests until it receives an ACK message. The requests are not removed unless and until, the remote target system gets an ACK message. Hence these requests take up or occupy valuable resources of the target machine.

To actually affect the target system, a large number of SYN bad IP packets have to be sent. As these packets have a Bad Source IP, they queue up, use up resources and memory or the target system and eventually crash, hang or reboot the system.

Land Attacks

A Land attack is similar to a SYN attack, the only difference being that instead of a bad IP Address, the IP address of the target system itself is used. This creates an infinite loop between the target system and the target system itself. However, almost all systems have filters or firewalls against such attacks.

Smurf Attacks

A Smurf attack is a sort of Brute Force DOS Attack, in which a huge number of Ping Requests are sent to a system (normally the router) in the Target Network, using Spoofed IP Addresses from within the target network. As and when the router gets a PING message, it will route it or echo it back, in turn flooding the Network with Packets, and jamming the traffic. If there are a large number of nodes, hosts etc in the Network, then it can easily clog the entire network and prevent any use of the services provided by it.

Read more about the Smurf Attacks at CERT: http://www.cert.org/advisories/CA-98.01.smurf.html

UDP Flooding

This kind of flooding is done against two target systems and can be used to stop the services offered by any of the two systems. Both of the target systems are connected to each other, one generating a series of characters for each packet received or in other words, requesting UDP character generating service while the other system, echoes all characters it receives. This creates an infinite non-stopping loop between the two systems, making them useless for any data exchange or service provision.

Distributed DOS Attacks

DOS attacks are not new; in fact they have been around for a long time. However there has been a recent wave of Distributed Denial of Services attacks which pose a great threat to Security and are on the verge of overtaking

Viruses/Trojans to become the deadliest threat to Internet Security. Now you see, in almost all of the above TCP/IP vulnerabilities, which are being exploited by hackers, there is a huge chance of the target's system administrator or the authorities tracing the attacks and getting hold of the attacker.

Now what is commonly being done is, say a group of 5 Hackers join and decide to bring a Fortune 500 company's server down. Now each one of them breaks into a smaller less protected network and takes over it. So now they have 5 networks and supposing there are around 20 systems in each network, it gives these Hackers, around 100 systems in all to attack from. So they sitting on there home computer, connect to the hacked less protected Network, install a Denial of Service Tool on these hacked networks and using these hacked systems in the various networks launch Attacks on the actual Fortune 500 Company. This makes the hackers less easy to detect and helps them to do what they wanted to do without getting caught. As they have full control over the smaller less protected network they can easily remove all traces before the authorities get there.

Not even a single system connected to the Internet is safe from such DDOS attacks. All platforms Including Unix, Windows NT are vulnerable to such attacks. Even MacOS has not been spared, as some of them are being used to conduct such DDOS attacks.

With this we come to the end of the first edition of DOS Attacked!!! Hope you liked this manual. This manual was an excerpt from the DOS attacked Tutorial, which was written exclusively for the HT Club. If you too are interested in receiving such manuals in the future, simply join the HT Club. On this note this is Ankit Fadia saying goodbye. J

Ankit Fadia
Ankit@bol.net.in