DEADLY DoS ATTACK

By Abhisek Datta
abhisek@programmer.net
http://www.hackersclub.up.to

Hello everybody.. I am back with another new exciting article of the HC series in the most happening topic of the current generation…
Well to start with I must say DoS (Denial of Service) attack is not at all hacking.. I repeat it is NOT hacking.. Any Script Kiddie can click some button to cause a deadly DoS attack which may bring down the servers of big big companies like Yahoo, Cnet. As I have read in some articles written by some legendary hackers where they mention about the change in the term Hacker. Today hacking seems to be quite different as that of past.. Today peoples who can creat a DoS gets fame and reputation in the Hacking World.. and are recognized as hackers.

Anyway to start with I must say that this article explain most of the commonly used DoS attack and we will take a clear look at the intricacies of these DoS attacks and how one can protect himself from these attacks..

What is a DoS attack ?

A Dos (denial of service) attack is a kinda attack which exploits an existing vulnerability in the operating system or in the softwares of the target machine or Internet Protocols like TCP/IP thus bringing down the aimed service or sometimes all the services of the target system. In short it prevents legitimate users to use the services offered by the target system. Well a very simple example of such attack is ping.. Previously in unpatched Win 95 systems TCP/IP protocols can only handle a data packet within the size of 64400 bytes.. thus a simple ping with the command line : ping –t –l 65500 <victim's IP> causes the system to crash or reboot.. its an example of the most simplest DoS used to be implemented in the previous days..

Nowadays this ping attack is quite lame cause almost all the operating systems are patched to prevent such attacks.. Nowadays advanced sophisticated attacks like SYN Flooding, Tear Drop, Smurf, TARGA3, Semirandom etc. are used. there are many more DoS techniques but I'll mension only those which are more or less assymetric in nature..(I'll explain it later)

There are generally two types of DoS attack.
1. Magic Packets Attack: In this attack an attacker causes a DoS by exploiting an existing vulnerability in the OS running in the target system or softwares of the target system by sending few specially designed data packets to particular ports. Example: Ping of Death, WinNuke.
Inside Info: well one more example I'll give about this kinda attack regarding Windows XP which I have recently discovered while a friend of mine was playing a 3D game in my computer.. it's the MEMORY DUMP bug.. you can say it is a vulnerability existing in Windows XP (I don't know about the previous versions) waiting to be exploited by intelligent and experienced Hackers.. In Windows XP what happens is that it uses a dump file (%systemroot%\MEMORY.dmp or c:\windows\MEMORY.dmp) to allocate some memory for debugging informations.. by default it is 64 KB.. if somehow remotely the size of this file is made to exceed 64 KB (considering that the user haven't change the default size limit of this file which is 64 KB) then the system will definitely reboot..

2**.Resource Exhaustion Attack:** Just as the name indicates this kinda attack depends on the fact that every computer system has definite amount of utilisable system resource. In this kinda attack the attacker sends unlimited amount of data packets in a special well planned method in an attempt to overload the system resource and the RAM of the target system thus compelling it to crash or hang or reboot.
Example: ICMP (Internet Control Message Protocol) Ping for network flood.

What is Asymmetric DoS ?

DoS attack can be implemented in a wide range of ways.. For example a T1 connection with a speed of around 10 Mega Bytes per second floods a network with a speed of only 56 kbps (as I have) then its quite obvious that the faster connection will easily flood the network lines of lesser bandwidth with data packets even by simple ping (considering he is in Unix OS.. cause windows does not allow sending of data packets larger than 64400 bytes).. But DoS attack can be performed in a very well planned sophisticated way in which a system with a bandwidth of as low as even 56kbps can bring down a system of very high bandwidth even 25 MBps..
For example if I send an ICMP ping request to a system in a network of considerable bandwidth with spoofed IP in such a way that the target systems thinks that the request is coming from a system within its network so as to compel it to send back the data packet to that particular system in its network thus causing a flood circle..
By repeating this process few times even from a 56 kbps dial up connection it is possible to bring down a network of high bandwidth cause a flood circle is developed within its internal network which will definitely overload the system resource..
It's a kinda Magic Packet with Resource Exhaustion attack.. pretty sophisticated and intelligent.. right ??? I guess and hope so.. ☺ Its called smurf attack. I'll explain it in details later on this article..

Now lets begin with the main part of this manual ie.. commonly used DoS attacks and how to execute them..

<u>SYN FLOODING</u>

This kind of DoS attack is executed by exploiting the TCP/IP 3 way handshake based authentication system. In this attack what happens, an attacker floods the target computer with unfinished SYN requests.. Since the victim computer cannot finish these SYN requests it has to use its system resource to store temporarily these SYN request thus slowly overloading the system resource and finally ending up by crashing it or rebooting it..

What is TCP/IP 3 way authentication system ?

Well to understand and execute SYN Flooding flawlessly and effectively you need to understand the very basic of this kind of attack which exploits the TCP/IP 3 way authentication system.. Now I am sure most of you might be asking what the hell is TCP/IP 3 way authentication system..never heard about it..
Did you ever wondered how authentication takes place when you dial up to your ISP requesting for a connection to your ISP (Internet Service Provider)..

For a successful connection between two computers.. Host and Client a complete and successful 3 way handshake must take place..

First the client send a SYN Packet (SYN request) to the Host asking for a TCP/IP connection.
Second the host replies with a SYN/ACK packet to the client thus indicating its response and acknowledgement..
Third the client sends an ACK packet to the host thus completing the connection..

Client ---------------------→ SYN ------------------------→Host   1st   Handshake
Host   --------------------→SYN/ACK--------------------→Client   2nd Handshake
Client----------------------→ACK-------------------------→Host   3rd Handshake

This is the very basis of connection establishment between two computers Host and Client.. At first this procedure is carried out then the username password authentication or any other form of authentication takes place..

Note: SYN packets, ACK Packets are special data packets designed by the Operating System.

Now I guess you have quite a lot idea about 3 way handshake system.. I guess its not that tough to understand.. Another thing you need to know is about the FIN packet.. Just like SYN,ACK packets FIN is also a specially designed data packet which is send by computer systems to terminate connections with one another..

How to perform practically a SYN Flooding ?

Well when you have the knowledge of this kind of attack I mean you know how this kind of attack takes place and what made it a kind of DoS attack.. Its easy to perform..
You need to flood the target computer with unfinished SYN requests.. By unfinished SYN requests I mean only SYN packets not any ACK packet in response with the host's SYN/ACK packet.. thus compelling it to crash or reboot..
Thinking practically, first I send a SYN packet requesting for a connection with the target system. Now the target system will definitely response with a SYN/ACK packet.. Now what I do is ignore this SYN/ACK packet from the host and I send a couple of more SYN request to the target system.. Firstly I have not completed the earlier 3 way handshake so the target system has a pending SYN packets which is loaded in its memory thus consuming system resource.. Secondly I send a couple of more SYN packets to the target system but did not response to the SYN/ACK packets from the host.. Thus slowly the resource of the target system is consumed by these pending SYN requests which are not being completed by me.. In this way I continued to flood the target system with thousands of SYN requests within a very short time. So what happens the target system's resource is slowly consumed by these pending SYN packets and ending up with a system crash or reboot thus Denying the services it was offering to its valid users..

Well I am sure you might be asking again how to send SYN,ACK packets to a target system and how to ignore SYN?ACK packet from the target system..Is there any tools for it ??
Yes there are a lot of tools which lets you to send custom made data packets..
Try out Libnet (search in google.com or in http://www.packetfactory.com)
You can also try a very good DoS tool which offers a varied range of DoS attacks..
It is TFN2k.. (again search at google.com ..dont ask me about the tools..)

TEARDROP ATTACK

This attack is also executed by exploiting a vulnerability present is almost all the Operating Systems.. The packet reassembling Vulnerability.. This is a very intelligent kind of attack which can be carried out from a system with very little bandwidth. It's a true example of asymmetric DoS.

What is Packet Reassembling Vulnerability ?

In explaining this vulnerability I am gonna give some practical example which will clarify all the intricacies of the packet reassembling vulnerability present in almost all the Operating System..
Say you have a 56 KBPS modem.. Now you want to send a file of around 1 MB to your friend through a direct connection as for example File Transfer in msn messenger, file transfer in AOL Instant Messenger, ICQ or by using FTP client-server.. Ever wondered how is it possible.. I mean you have a modem which had a capacity of only 56 Kilobytes per second of data transfer.. Now how come it is gonna transfer a file of 1 MB.. The answer is quite simple.. What actually happens is that the file is broken down into small fragments at the source system know as packets and all these packets are assembled at the target system to produce the original file..
Every packets of data which are send through the internet has two parts..

1. The Head Part : This part contains some important infos like sequence number, byte length, data type etc..
2. The Tail Part : It contains the actual information stored in the file..

The head part contains the info for reassembling..
Lets take a small example:
Say I wanna send a file of size 3000 KB to a friend of mine..
Now what happens this file is split up into say 3 parts each containing 1000 KB

Note: In practice the original fileis split up into much smaller parts.. I have sayed 3 parts only to avoid complications in explanation

Now these 3 parts are called data packets and each packet will carry 1000 KB..
The header part of the first packet will have a bye length of 1 – 1000
Similarly the header part of second and third packet will have a byte length of 1001-2000 and 2001-3000..
Now each packet has an OFFSET field which indicates which bye to which byte a particular data packet contains… Now according to this OFFSET field the data packets are reassembled in the target system to generate the original file..

The header part of the data packets in the above stated file transfer can be explained schematically as :

Data Packet No.	Size	OFFSET FIELD	Type
1	1000	1-1000	TCP/IP
2	1000	1001-2000	TCP/IP
3	1000	2001-3000	TCP/IP

How to perform TEARDROP Attack ?

As for now I guess you are acquainted with packet reassembling system..

In case of teardrop attack this system is exploited..
In TearDrop attack custom made data packets with confusing OFFSET fields are send to the target system thus ending it up in system crash or reboot..

First I want to send a file of size say 5000 KB to the target system and the file is split up into 5 data packets each carrying 1000 KB at my end which is supposed to be reassembled in the target system.. For executing the teardrop attack on the target system I have to modify the OFFSET field of these data packets which will be send to the target system where the target system will attempt to reassemble it according to the OFFSET field..

Say the first packet will have a OFFSET field of 1-1000.. then 1001-2000 now I play the trick from the third packet onwards. I send the third packet with an OFFSET field of 2000-3000 , the fourth with 3000-4000 and the fifth with 4000-5000.. I am sure most of you have noticed that 2000,3000,4000 has appeared twice in the OFFSET field of the data packets send to the target system.. The target system will expect something like :
1 --→ 1000
1001 --→ 2000
2001 --→ 3000
3001 --→ 4000
4001 --→ 5000

but actually it is getting something like:
1 ---→ 1000
1001 ---→ 2000
2000 ---→ 3000
3000 ---→ 4000
4000 ---→ 5000

The target system will have no idea as how to handle this kind of data packets and reassembling this data packets according to TCP/IP or Ipv4 will result in system crash or reboot..

Tools to use: Again you can try Elite or TFN2K.. or if you're a expert programmer in C or any other language then go for making your own program..

SMURF ATTACK

Well this is really an interesting example of asymmetric DoS attack. I think it's a very smart, intelligent and sophisticated attack but has the capacity of causing a quake in the target network thus bringing down the entire network. Well what happens in this kind of attack is that an attacker uses simple ping flood with spoofed IP and tries to create a circle of flood among the target system and a system within its internal network.. I agree this is a little complicated to understand but its really usefull.. however the target computer may be secure and protected, it can be brought down with a well planned smurf attack.
To deal with this kind of attack you need to know and have a clear conception about IP Spoofing. I agree that IP spoofing may be new to you. In plain words IP Spoofing means to amend your IP with some other IP. For example my IP is 203.192.27.45 . By performing IP Spoofing I can establish a connection or send data packets to a remote system with some other IP say 64.4.44.8 (Probably Hotmail's IP).. In plain and simple words IP spoofing means to bluff your IP to a remote system.

But wait a second.. aint it cool if the subject of IP Spoofing is so plain and simple as it seems to be and also regarded by some people.. I don't know about other but practically I feel IP Spoofing is really a complicated subject but one of the most important in hacking.. The most important reason for it being so complicated is because it is a blind attack. You cannot actually see or realize what is the result of your actions on the target system.
To know more about IP Spoofing go through the article called "IP Spoofing Demystified" available in the books sections of http://blacksun.box.sk

Anyway I think I should give a little overview on IP Spoofing though I don't think I am an expert in the subject.

What is IP Spoofing ?

Well as I have explained IP Spoofing in simple before in this article I don't want to repeat it anymore. Here I want to explain its intricacies.
As I have explained earlier in this manual about the TCP/IP 3 way handshake authentication system. Another thing I need to say is that the header part of every data packet consists of a sequence number which is particular to that packet only. This sequence number helps the target system to distinguish that particular data packet.. They can be realized as 32 bit counters ranging between 0 to 4,294,967,295
Well in IP Spoofing what happens in order to establish a connection with a remote system with spoofed IP you need to send custom made data packets to the target system. According to the TCP/IP 3 way handshake authentication system, in response to your SYN packets the target computer will send a SYN/ACK packet to the spoofed IP.
For example:

```
     Real:    203.197.48.1       SYN          64.4.44.1
Attacker ------------------------------------------------→ Target
   Spoofed: 203.197.44.250    SYN          64.4.44.1

 IP: 64.4.44.1                 SYN/ACK                IP:203.197.44.250
Target   ------------------------------------------------→ Spoofed IP
```

Well now as you see in order to complete the TCP connection with the spoofed IP you need to send an ACK packet to the target system with a valid sequence number to establish the connection which is a real tough job. Anyway full explanation of IP Spoofing and sequence numbers and its implementations are beyond the scope of this manual. Read "IP Spoofing Demystified" [http://blacksun.box.sk] for more details..

IMPLENTATION OF SMURF ATTACK

So far now I think you know the basic overview of smurf attack. In this kind of attack what happens an attacker continuously ping floods the target system with an IP spoofed as the IP of a system within the internal network of the target computer. So what happens in response to your ping requests the target computer sends data packets to the spoofed IP ie. the system within its internal network which causes that system to resend it to our target system. So what happens our target system is being ping flooded from two ends and in one end a circle of ping of death is established which results in resource exhaustion of the target system resulting in system crash.

A WELL PLANNED DoS ATTACK

In here I am going to figure out some interesting methods of implementing a successful DoS attack.. Well I must agree the fact that I once thought of executing this method to the web server of one big company.. but finally end up when my father came to know about it and threatened me by telling that he will throw out me an my computer from the house..
Hence it is totally a plan of mine and I never practically verified its validity..

To start with I must say that whatever I do I always know what the hell I am doing. I don’t act like stupid script kiddies and get busted.. though I must agree I am not into real hacking.. First and foremost thing which comes in my mind is your security.. Say you executed a brilliant DoS attack which causes havoc in your target network but finally you end up spending days in government expense.. you got busted pal.. The only reason was that you don’t know what you were doing.. Next day in your news paper you will find a news like ‟ Hacker got caught for DoS ‟.. this seems to be pretty cool info for you and your friend.. But do you know how a real hacker will write this news.. he’ll write ‟ A Stupid script clicked some button and caused a DoS and since he doesn’t know what he was doing, he got busted ‟ . I guess it aint cool..

Now to begin with, say you tried to execute a SYN Flooding on your ISP’s web server. Ok, your lucky enough and somehow you managed to crash your target system but to your utter unconsciousness you forgot to remove the entries in their logs that you left while sending SYN packets or you lack the knowledge about how to remove entries.. generally IIS logs are kept in the folder: C:\Inetpub\wwwroot_vti_log ..
Generally you can try cross site scripting in order to remove logs.. Though this method is quite lame and old and in most cases don’t work.. A cross site scripted attack URL looks like:
http://ISP.net/../../../../%systemroot%\system32\cmd.exe?del%20 C:\Inetpub\wwwroot_vti_log*.txt

This is just one method.. There are many other methods.. Generally experienced hackers aims at getting root on un protected systems associated with the main server and then attempting some kinds backdoor installation to the main system..

Now to me what I think a well planned DoS attack is the one in which you’re going to laid down the server simultaneously keeping yourself in the safe side thus protecting yourself from getting busted..
Well what I feel like doing is using shell accounts which allows uploading and installation of custom tools.. I guess you are familiar with shell accounts. These are accounts on a Unix based machines offered as a service by many website like http://freeshells.org which lets you use the resources of the Unix system in the server from your windows system using telnet and by logging into your account..
If you have a shell account like this you can try uploading your tools there and launching your attack from their server thus keeping yourself in the safe side..

Protection From DoS Attacks

Just like the attackers who are finding vulnerabilities to be exploited for causing a DoS attack the programmers of the softwares and particularly and most importantly Operating System are releasing patches for preventing such kind of attacks.. For example Microsoft has patched its OS to prevent SYN Flooding by limiting the number of SYN requests to be stored in the system memory thus preventing it from getting overloaded.. Well this is just one case.. SYN flooding can be executed in many ways and may be also be introduced in many ways in future which these patches wont be able to prevent.. So I think along with updating your softwares and Operating System with patches from its developers it is necessary to know about the attack which is being carried out against you and the vulnerability at your end which is being exploited.. so in order to prevent such attacks..

Oki Doki everybody…
That’s it for now..

Its time to say bye for now…
Please let me know about your comments..

Abhisek Datta
abhisek@programmer.net
http://hackersclub.up.to

Fear them not therefore: for there is nothing covered, that shall not be revealed; and hid, that shall not be known"
Matthew 10:26