Dos Attacks Explained
By Amin Nagpure.(sukhoi) / 4/8/99.

----Disclaimer---
Writer don't intend to get information by his writing to be used in an illegal way ,don't do it, if you get caught then you have yourself to blame. My information is just for educational purpose only.

This tutorial is written for absolute newbies who don't know whats dos attack , technical details is reduced so that basic concept about what it is get cleared.ok
So don't email me and say you lack technical knowledge or your tutorial is less in it. There are so many available on the net. This one is for absolute newbie okay.

Dos attacks-"Denial of Service" Attack
It's the attack to deny the service to the legitmate user ,so that he suffers there are several reasons to do that.
Mostly likely reason is 'NAST-YINESS'

Okay there are two ways for dos attacks one is the lame way and the other is the elite way

Lame way

Email Bombs – it s the technique in which a person email Alc is flooded with emails, it's the lamest form of DOS attack. All a person has to do is go on the net get some email bomber like UNA or KABOOM put the victims address and there ya go , his email address will be flooded with the unwanted emails, there is also another way put his email address into some porn subscription he will get bombed without you doing anything ,LOL
When the victims email alc gets flooded he has a pain in differentiating and deleting the unwanted emails and it's the huugee task.
And if the victim is the admin of the server and his email alc there is flooded it also looses his disk space.

Continous login – suppose a server is configured to allow only specified amount login attempts then ,and you know his username you can lock his account, by attempting to connect by his name to the server which will lock his account and there ya go , the legitmate user wont be able to log in ,the reason, you locked his Alc.

Okay now the neophyte way, its not that elite way but some what better than the lame way, atleast you are doing something technical.

Syn Flooding
This is a exploit in tcp/ip method of handshake .
Read some basics on tcp/ip okay lets start.

Normal way :-
Syn-packet is sent to the host by the client who intends to establish a connection

SYN
Client ----------→ Host

Then in the second step host replies with syn/ack packet to the client

SYN/ACK
Client ←----------Host

Then in the third and the last step
Client replies with ack packet to the host and then the threeway handshake is complete

Okay got it now ..?

Now in attack
Several syn packet is sent to host via spoofed ip address(bad or dead ip addresses) now then what happens the host replies with syn/ack packet and host waits for the ack packet. But however the ip address don't exist it keeps waiting ,thus it queues up and eats the system resources and thus causes the server to crash or reboot.

Land attack
A land attack is similar to syn attack but instead of bad ip address the ip address of the target system itself is used. This creates an infinite loop , and the target system crashes. But however almost all systems are configured against this type of attacks.

Smurf Attack
A smurf attack is a sort of brute force dos attack , in which a huge number normally the router using the spoofed ip address from within the target network , so when it gets the ping it echos it back causing the network to flood. Thus jamming the traffic

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.

Ping of death

This Attack don't work now as all the servers are patched against this type of attack
In this attack a target system is pinged with data packet exceed the normal size allowed by the tcp/ip i.e 65536. this will cause the system to reboot or hangup.

Tear Drop

When the data is passed from one system into another it is broken down into smaller fragments, and then in the reciving host they are again reassembled .
These packets have an offset field in there TCP header part which specifies from which part to which part that data carries or the range of data that it is carrying. This along with the sequence numbers, this helps the receiving host to reassemble the data.

In tear drop the packets are sent with the overlapping offset field values thus the reciveing host is unable to reassemble them and crashes.

There is new trent called DDOS attack where several computers mostly (hacked computers) for dos attacks.
More on this later.

bye