brigante.sytes.net

-: Denial Of Service (DoS) Attacks :-

A denial of service (DoS) attack is an attack that clogs up so much memory on the target system that it can not serve it's users, or it causes the target system to crash, reboot, or otherwise deny services to legitimate users.There are several different kinds of dos attacks as discussed below:-

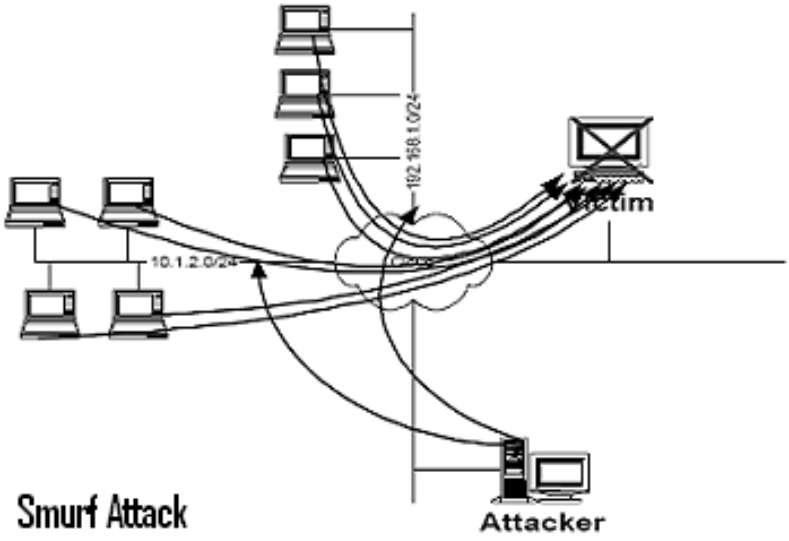
1) Ping Of Death :- The ping of death attack sends oversized ICMP datagrams (encapsulated in IP packets) to the victim.The Ping command makes use of the ICMP echo request and echo reply messages and it's commonly used to determine whether the remote host is alive. In a ping of death attack, however, ping causes the remote system to hang, reboot or crash. To do so the attacker uses, the ping command in conjuction with -l argument (used to specify the size of the packet sent) to ping the target system that exceeds the maximum bytes allowed by TCP/IP (65,536).
example:- c:/>ping -l 65540 hostname
Fortunately, nearly all operating systems these days are not vulnerable to the ping of death attack.

2) Teardrop Attack :- Whenever data is sent over the internet, it is broken into fragments at the source system and reassembled at the destination system. For example you need to send 3,000 bytes of data from one system to another. Rather than sending the entire chunk in asingle packet, the data is broken down into smaller packets as given below:
* packet 1 will carry bytes 1-1000.
* packet 2 will carry bytes 1001-2000.
* packet 3 will carry bytes 2001-3000.
In teardrop attack, however, the data packets sent to the target computer contais bytes that overlaps with each other.
(bytes 1-1500) (bytes 1001-2000) (bytes 1500-2500)
When the target system receives such a series of packets, it can not reassemble the data and therefore will crash, hang, or reboot.
Old Linux systems, Windows NT/95 are vulnerable.

3) SYN - Flood Attack :- In SYN flooding attack, several SYN packets are sent to the target host, all with an invalid source IP address. When the target system receives these SYN packets, it tries to respond to each one with a SYN/ACK packet but as all the source IP addresses are invalid the target system goes into wait state for ACK message to receive from source. Eventually, due to large number of connection requests, the target systems' memory is consumed. In order to actually affect the target system, a large number of SYN packets with invalid IP addresses must be sent.

4) Land Attack :- A land attack is similar to SYN attack, the only difference being that instead of including an invalid IP address, the SYN packet include the IP address of the target sysetm itself. As a result an infinite loop is created within the target system, which ultimately hangs and crashes.Windows NT before Service Pack 4 are vulnerable to this attack.

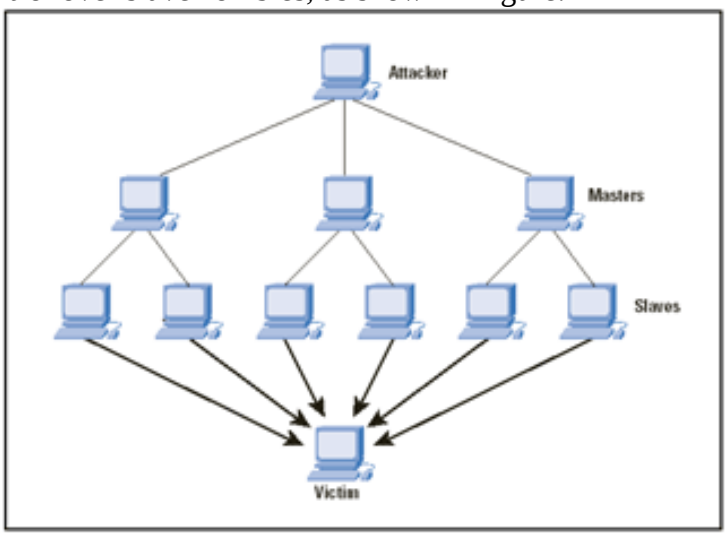
5) Smurf Attack :- There are 3 players in the smurf attack–the attacker,the intermediary (which can also be a victim) and the victim. In most scenarios the attacker spoofs the IP source address as the IP of the intended victim to the intermediary network broadcast address. Every host on the intermediary network replies, flooding the victim and the intermediary network with network traffic.



Result:- Performance may be degraded such that the victim, the victim and intermediary networks become congested and unusable, i.e. clogging the network and preventing legitimate users from obtaining network services.

6) UDP - Flood Attack :- Two UDP services: echo (which echos back any character received) and chargen (which generates character) were used in the past for network testing and are enabled by default on most systems. These services can be used to launch a DOS by connecting the chargen to echo ports on the same or another machine and generating large amounts of network traffic.

7) Distributed Denial Of Service (DDoS) :- In Distributed DoS attack, there are 100 or more different attackers (systems) attacking the single system. Due to higher number of attackers DDoS attack is more effective and dangerous than regular DoS attack. The attackers have control over master zombies, which, in turn, have control over slave zombies, as shown in figure.



No system connected to the internet is safe from DDoS attacks. All platforms, including Unix and Windows NT, are vulnerable to such attacks. Even Mac OS machines have been used to conduct DDoS attacks.

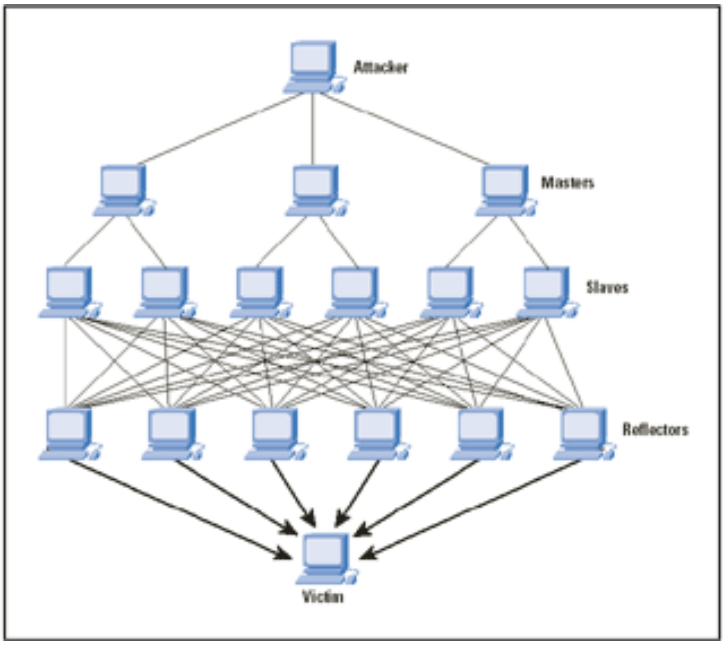
The most popular DDoS tools are:-

a) Trin00 (WinTrinoo)
b) Tribe Flood Network (TFN) (TFN2k)

c) Shaft
d) Stacheldraht
e) MStream

8) Distributed Denial Of Service with Reflectors (DRDoS) :- In DRDoS attacks the army of the attacker consists of master zombies, slave zombies, and reflectors. The difference in this type of attack is that slave zombies are led by master zombies to send a stream of packets with the victim's IP address as the source IP address to other uninfected machines (known as reflectors), exhorting these machines to connect with the victim. Then the reflectors send the victim a greater volume of traffic, as a reply to its exhortation for the opening of a new connection, because they believe that the victim was the host that asked for it. Therefore, in DRDoS attacks, the attack is mounted by noncompromised machines, which mount the attack without being aware of the action.

a DRDoS attack creates a greater volume of traffic because of its more distributed nature, as shown in the figure below.



source: http://www.insecure.in/dos_attacks.asp

more free stuff, resources, tuts, articles, free e-books: http://brigante.sytes.net