Teardrop Attack

A Teardrop attack occurs when an attacker sends fragments with overlapping values in their offset fields, which then cause the target system to crash when it attempts to reassemble the data. It affects systems that run Windows NT 4.0, Windows 95, and Linux up to 2.0.32, causing them to hang, crash, or reboot.

As stated earlier, TCP/IP will fragment a packet that is too large into smaller packets, no larger than 64 kilobytes. The fragment packets identify an offset from the beginning of the original packet that enables the entire original packet to be reassembled by the receiving system. In the Teardrop attack, the attacker manipulates the offset value of the second or latter fragments to overlap with a previous fragment. Since older operating systems are not equipped for this situation, it can cause them to crash.

SYN Flooding Attack

SYN flooding occurs when the intruder sends SYN packets (requests) to the host system faster than the system can handle them.

A connection is established through a TCP three-way handshake, in which the following occurs:

1. Host A sends a SYN request to Host B.
2. Host B receives the SYN request and replies to the request with a SYN-ACK to Host A.
3. Host A receives the SYN-ACK and responds with an ACK packet, establishing the connection.

When Host B receives the SYN request from Host A, it makes use of the partially open connections that are available on the listed line for at least 75 seconds.

The intruder transmits large numbers of such SYN requests, producing a TCP SYN flooding attack. This attack works by filling the table reserved for half-open TCP connections in the operating system's TCP/IP stack. When the table becomes full, new connections cannot be opened until some entries are removed from the table due to a handshake timeout. This attack can be carried out using fake IP addresses, making it difficult to trace the source. The table of connections can be filled without spoofing the source IP address. Normally, the space existing for fixed tables, such as a half-open TCP connection table, is less than the total.

LAND Attack

In a LAND attack, an attacker sends a fake TCP SYN packet with the same source and destination IP addresses and ports to a host computer. The IP address used is the host’s IP address. For this to work, the victim’s network must be unprotected against packets coming from outside with their own IP addresses. When the target machine receives the packet, the machine considers that it is sending the message to itself, and that may cause the machine to crash.

The symptoms of a LAND attack depend upon the operating system running on the targeted machine. On a Windows NT machine, this attack just slows the machine down for 60 seconds, while Windows 95 or 98 machines may crash or lock up. UNIX machines also crash or hang and require a reboot.

Because LAND uses spoofed packets to attack, only blocking spoofed packets can prevent it. Still, with current IP technology, it is not possible to completely filter spoofed packets.

Smurf Attack

The smurf attack, named after the program used to carry it out, is a network-level attack against hosts. The attacker sends a large amount of ICMP echo (ping) traffic to IP broadcast addresses using a spoofed source address matching that of the victim. Smurf attacks generate a large number of echo responses from a single request, which results in a huge network traffic jam, causing the network to crash. If the routing device delivering traffic to those broadcast addresses accepts the IP broadcast, hosts on that IP network will take the ICMP echo request and reply to each echo, exponentially increasing the replies.

On a multiaccess broadcast network, there could potentially be hundreds of machines replying to each packet, ensuring that the spoofed host may no longer be able to receive or distinguish real traffic.

Fraggle Attack

The fraggle attack is a UDP variant of the Smurf attack. In Fraggle attacks, an attacker sends a large number of UDP ping packets, instead of ICMP echo reply packets, to a list of IP addresses using a spoofed IP address. All of the addressed hosts then send an ICMP echo reply, which may crash the targeted system. Fraggle attacks