Introduction to Investigating DoS Attacks

In denial-of-service attacks, or DoS attacks, attackers attempt to prevent legitimate users of a service from using it by flooding the network with traffic or disrupting connections. The attacker may target a particular server application (HTTP, FTP, ICMP, TCP, etc.) or the network as a whole. There may also be an effort to interrupt the connection between two machines, preventing or disturbing access to a particular system or individual. Improper use of resources may also create a DoS. For example, an intruder may use an unidentified FTP area to store large amounts of data, using disk space and producing network traffic problems.

In such an attack, a user or organization is deprived of the services of a resource that they would normally expect to have. In general, for certain network services, failure might mean the loss of a service such as e-mail or a Web server. DoS attacks are a kind of security breach that does not generally result in the theft of information or in any other type of security loss, but these attacks can harm the target in terms of time and resources.

Indications of a DoS/DDoS Attack

Indications of a DoS/DDoS attack are as follows:

- **Unusual slowdown of network services**: Most low- and medium-risk DoS attacks only slow down network services. They do not completely prevent access; they just make it more difficult.
- **Unavailability of a particular Web site**: When a DoS attack occurs against a poorly protected system or network server for any site, it can make the site impossible to reach.
- **Dramatic increase in the volume of spam**: Spam e-mails are sometimes used to generate huge amounts of bogus traffic over the network, causing a DoS.

Types of DoS Attacks

The main types of DoS attacks are as follows:

- **Ping of death**: Sending a malformed or otherwise malicious ping to a computer
- **Teardrop**: Forging fragmented packets designed to overlap each other when the receiving hosts defragment them
- **SYN flooding**: Sending TCP connection requests to a target host faster than it can process them
- **LAND**: Sending a data packet to a targeted machine with the same host and port names for the source and the destination
- **Smurf**: Using spoofed IP addresses to send broadcast ping messages to a large number of hosts in a network to flood the system
- **Fraggle**: Using UDP packets to flood a network
- **Snork**: Targeted against Windows NT RPC services
- **OOB attack**: Exploiting a bug in Microsoft’s implementation of its IP stack
- **Buffer overflow attack**: Sending more information to a program than it is allocated to handle
- **Nuke attack**: Repeatedly sending fragmented or invalid ICMP packets to the target computer
- **Reflected attack**: Sending false requests to a large number of computers, which respond to those requests

Ping of Death Attack

In the ping of death attack, an attacker deliberately sends an ICMP (Internet Control Message Protocol) echo packet of more than 65,536 bytes, the largest size acceptable by the IP protocol. Fragmentation is one of the features of TCP/IP, requiring that a large IP packet be broken down into smaller segments. Many operating systems do not know what to do when they receive an oversized packet, so they freeze, crash, or reboot.

Ping of death attacks are dangerous since the identity of the attacker sending the huge packet could simply be spoofed. Also, the attacker does not have to know anything about the target except its IP address. Several Web sites block ICMP ping messages at their firewalls to avoid this type of DoS attack.