How a Hacker Can Attack in your network

A paper by Dr. Ajay Data , CEO, Data Ingenious Global Ltd

What is Denial-of-Service (DoS) Attacks

• Ping of death – Sends an invalid fragment, which starts before the end of packet, but extends past the end of the packet.

• Syn Flood – Sends TCP SYN packet (which starts connections) very rapidly, leaving the attacked machine waiting to complete a huge number of connections, and causing it to run out of resources and start dropping legitimate connections. A new defense against this is “SYN cookies.” Each side of a connection has its own sequence number. In response to a SYN, the attacked machine creates a special sequence number that is a “cookie” of the connection, then “forgets” everything it knows about the connection. It can then recreate the forgotten information about the connection when the next
packets come in from a legitimate connection.

• Loop – Sends a forged SYN packet with identical source/destination address/port so that the system goes into an infinite loop trying to complete the TCP connection. System Configuration Holes Weaknesses in enterprise system configuration can be classified as follows:

To execute a Denial-of-Service (DOS) attack, a hacker uses Trojans to take control over a potentially unlimited number of zombie computers, which then take aim at a single target and flood it with traffic in an attempt to overwhelm the server.

• Default configurations – Most systems are shipped to customers with default, easy-to-use configurations. Unfortunately, “easy-to-use” can mean “easy-to-break-into” as well. Almost any UNIX or WinNT machine shipped can be exploited rather easily.

• Empty/Default root passwords – A surprising number of machines are configured with empty or default root/administrator passwords. One of the first things an intruder will do on a network is to scan all machines for empty passwords.

• Hole creation – Virtually all programs can be configured to run in a non-secure mode which can leave unnecessary holes on the system. Additionally, sometimes administrators will inadvertently open a hole on a machine. Most administration guides will suggest that administrators turn off everything that doesn't absolutely need to run on a machine in order to avoid accidental holes. Unfortunately this is easier said than done, since many administrators aren’t familiar with disabling many common services. Exploiting Software Issues Software bugs can be exploited in the server daemons, the client applications, the operating system, and the network stack. Software bugs can be classified in the following manner:

• Buffer Overflows – Almost all the security holes you read about in the press are due to this problem. A typical example is a programmer who will set aside a specific number of characters to hold a login username. Hackers will look for these types of vulnerabilities, often sending longer strings than specified, including code that will be executed by the server. Hackers find these bugs in several ways. First, the source code for a lot of services is available on the net. Hackers routinely look through this code searching for programs that have buffer limitations. Hackers will also examine every place the program accepts input and try to overflow it with random data. If the program crashes, there is a good chance that carefully constructed input will allow the hacker to break into the system.