Denial of Service (DoS) Attacks

A Denial of Service (DoS) attack is one that attempts to prevent the victim from being able to use all or part of his/her network connection.

A denial of service attack may target a user to prevent him/her from making outgoing connections on the network. It may also target an entire organization to either prevent outgoing traffic or to prevent incoming traffic to certain network services, such as the organizations web page.

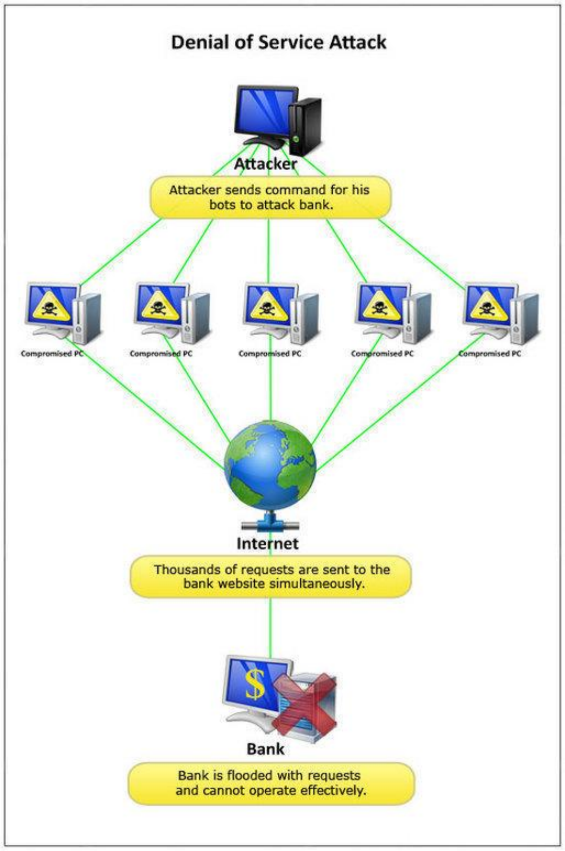
Denial of service attacks are much easier to accomplish than remotely gaining administrative access to a target system. Because of this, denial of service attacks have become very common on the Internet.

Types of Denial of Service (DoS) Attacks

These are a few of the classic denial of service attacks. Most of these rely on weaknesses in the TCP/IP protocol. Vendor patches and proper network configuration have made most of these denial of service attacks difficult or impossible to accomplish.

Flood Attack

The earliest form of denial of service attack was the flood attack. The attacker simply sent more traffic than the victim could handle. Flood attacks required the attacker to have a faster network connection than the victim. This is the lowest-tech of the denial of service attacks and also the most difficult to completely prevent.


Denial of Service Attack
Attacker
Attacker sends command for his bots to attack bank.
Compromised PC
Compromised PC
Compromised PC
Compromised PC
Compromised PC
Internet
Thousands of requests are sent to the bank website simultaneously.
Bank
Bank is flooded with requests and cannot operate effectively.

Ping of Death Attack

The Ping of Death attack relied on a bug in the Berkeley TCP/IP stack, which also existed on most systems that copied the Berkeley network code. The ping of death simply sent ping packets larger than 65,535 bytes to the victim. This denial of service attack was as simple as:

```
ping -l 86600 victim.org
```

SYN Attack

In the TCP protocol, handshaking of network connections is done with SYN and ACK messages. The system that wishes to communicate sends a SYN message to the target system. The target system then responds with an ACK message. In a SYN attack, the attacker floods the target with SYN messages spoofed to appear to be from unreachable Internet addresses. This fills up the buffer space for SYN messages on the target machine, preventing other systems on the network from communicating with the target machine.

Teardrop Attack

The Teardrop Attack uses the IP's packet fragmentation algorithm to send corrupted packets to the victim machine. This confuses the victim machine and may hang it.

Smurf Attack

In the Smurf Attack, the attacker sends a ping request to a third party's broadcast address on the network. This ping request is spoofed to appear to come from the victim's network address. Every system within the third party's broadcast domain then sends ping responses to the victim.

Distributed Denial of Service (DDoS) Attacks

A Distributed Denial of Service (DDoS) attack is a denial of service attack that is mounted from a large number of locations across the network.

DDoS attacks are usually mounted from a large number of compromised systems. A trojan horse, a worm, or manual hacking may have compromised these systems.
These compromised systems are usually controlled with a fairly sophisticated piece of client-server software such as Trinoo, Tribe Flood Network, Stacheldraht, TFN2K, Shaft, and Mstream.

The Mydoom worm attempted DDoS attacks against SCO and Microsoft from the systems that it infected.
DDoS attacks can be very difficult to defend against.

Source: http://www.tech-faq.com/denial-of-service-dos-attacks.html