

Denial of service attacks. An overview

Denial of Service Attack (DoS)

Attack whose primary purpose is to prevent legitimate use of the computer or network.

- Prevent authorized access to resources
- Delay time critical operations
- Degradation of service

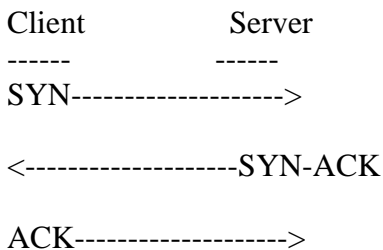
Modes of Attack

- Consumption of scarce resources:
 - To prevent hosts or networks from communicating on the network
 - Does not depend on the attacker being able to consume your network bandwidth. But for example, the intruder consumes kernel data structures involved in establishing a network connection (SYN flooding). Other resources are disk space (E-mail bombing, FTP etc)
 - Using your own resources against you. Legitimate service of a host used in unexpected ways (UDP packet storm)
 - Bandwidth consumption: Consume all available bandwidth on your network by generating a large number of packets directed to your network (ICMP ECHO ping flooding).
- Destruction or alteration of Configuration information:
 - An improperly configured computer may not perform well or not operate at all
 - Examples: Intruder changes routing information, modify Win NT registers etc.
- Physical destruction or alteration of network components:
 - Attack on system's physical security
 - Unauthorized access to computers, network closets, power and cooling components of the network.

Types of DoS attacks

- TCP SYN Flooding (with IP spoofing)

The client system begins by sending a SYN message to the server. The server then acknowledges the SYN message by sending SYN-ACK message to the client. The client then finishes establishing the connection by responding with an ACK message. The connection between the client and the server is then open, and the service-specific data can be exchanged between the client and the server. Here is a view of this message flow:



Client and server can now send service-specific data.

The potential for abuse arises at the point where the server system has sent an acknowledgment (SYN-ACK) back to client but has not yet received the ACK message. This is what we mean by half-open connection. The server has built in its system memory a data structure describing all pending connections. This data structure is of finite size, and it can be made to overflow by intentionally creating too many partially-open connections.

Creating half-open connections is easily accomplished with IP spoofing. The attacking system sends SYN messages to the victim server system; these appear to be legitimate but in fact reference a client system that is unable to respond to the SYN-ACK messages. This means that the final ACK message will never be sent to the victim server system.

The half-open connections data structure on the victim server system will eventually fill; then the system will be unable to accept any new incoming connections until the table is emptied out.

Safeguard:

Currently, the best method is to install a filtering router that restricts the input to your external interface (known as an input filter or ingress filter) by not allowing a packet through if it has a source address from your internal network. In addition, you should filter outgoing packets that have a source address different from your internal network to prevent a source IP spoofing attack from originating from your site.

- UDP packet storm (or Magnification- Fraggle, PingPong)

A UDP magnification attack relies on the existence of several standard, but generally unused UDP services:

- The chargen (character generation) service. This is a UDP port that, when connected to, generates a constant stream of data, and
- The echo service. This is a UDP port that simply echos the source packet (with source and destination addresses reversed).

Safeguard:

Disable all unnecessary UDP services (including daytime, chargen, and echo) on host machines. As a general rule: if you don't need it, disable it. Also, block UDP requests to low-numbered ports originating from non-ephemeral (ports 1024 and below) port numbers at your external router.

- ICMP Echo or Ping Flooding

One of the simplest methods. Uses common diagnostic tool “ping”. Ping sends an ICMP Echo to a host which responds with an ICMP Echo Reply.

In the Ping Flooding attack, attacker floods victim with IP Ping Packets.

Safeguard

Configure your OS to have a threshold when it receives ping requests. Or block them at the firewall. However the upstream network link can become congested just by the Ping requests.

- Others are E-mail bombing and Spamming

Use anti-spam filters and gateways. Not very effective though.

Distributed Denial of Service (DdoS)

- ICMP Echo or Ping Flooding (Smurf)

An ICMP magnification attack (or Smurf) uses ICMP Echo (ping) packets to generate multiple ICMP Echo Replies. By constructing an ICMP Echo request with a spoofed source address (the target), and a broadcast-directed destination, a single ICMP Echo packet could potentially generate an ICMP Echo Response from each host on a given subnet. An attacker with a fast connection can use this multiplication effect to completely saturate the bandwidth of the target host. We used to see this type of traffic from our Internet Service Provider quite regularly.

There are three parties involved in an ICMP magnification.

- The Attacker, who generates spoofed ICMP packets on a given subnet
- The Intermediates, who's network hosts reply to the packets, and contribute to the magnification, and
- The Target, who received ICMP echo replies from the Intermediates.

Safeguard

There's unfortunately not much you can do. Though it is possible to block the offending packets at your external router, the bandwidth upstream of that router will remain blocked. It takes coordination with your upstream provider to block the attacks at the source.

To prevent someone at your site from initiating a Smurf attack, configure your external router to block all outbound packets from your site that indicate a source address not contained within your subnet block. If the spoofed packet can't get out, it can't do much harm.

To avoid being an intermediary, and contributing to somebody else's Denial of Service attempt, configure your router to block all network-prefix-directed broadcast packets. That is, disallow broadcast ICMP packets in through your router. This will allow you to retain the ability to perform a broadcast-directed ping inside your network (which is occasionally useful for diagnostic purposes), while eliminating an outsider's ability to exploit this behaviour. If you're truly worried, you may also wish to configure your host machines to ignore ICMP broadcasts entirely.

- Application Packet Magnification – NetQuake

Any network-based application that generates multiple responses to a single packet can be used for this purpose. A good example of this was seen recently involving NetQuake servers. If an appropriately formed Hello3 packet is sent to a NetQuake servers, the server will respond with a series of Connect attempts, approximately one per second. If sent from a spoofed (target) address, and sent to the approximately 400 NetQuake servers out there, a sustained UDP stream can be generated.

This technique can be applied to any network application that assists in this multiplication effect.

Safeguard

Not much you can do, since it is very application specific.

- Trinoo

"Trinoo" (a.k.a. "trin00") master/slave programs, which implement a distributed network denial of service tool.

- Trinoo master program called a handler
- Installed on compromised machine
- Automates control of agent programs
- List of agents (their IP address). Agents are installed on other compromised machines.
- Attacker logs in to handler in order to start the attack
- Usually attacks are UDP flooding
- Usually agents IP is not spoofed. Thus agents can be found easily. But it is usually too late

- Tribe Flood Network (TFN2K)

TFN, much like Trinoo, is a distributed tool used to launch coordinated denial of service attacks from many sources against one or more targets. In addition to being able to generate UDP flood attacks, a TFN network can also generate TCP SYN flood, ICMP echo request flood, and ICMP directed broadcast (e.g., smurf) denial of service attacks. TFN has the capability to generate packets with spoofed source IP addresses.

Safegurads:

Prevention is not straight forward because of the interdependency of site security on the Internet; the tools are typically installed on compromised systems that are outside of the administrative control of eventual denial of service attack targets.

- Staheldraht

Based on Trinoo/TFN concept. However it is more sophisticated.

- Encrypted communication between attacker and master program
- Automated updates of agent programs
- Multiple types of attack
- Generate packets with spoofed IP address

Safegurads for DDoS

- Install IDS systems (both HIDS and NIDS)
- Firewall in place
- Correctly configured routers (Ingress filters)
- Virus scanners
- Policy for disaster recovery
- Redundant servers and equipment
- Disable any unused network services
- Enable quota
- Install patches to guard against TCP/SYN (syncookies Linux)