Software Engineering Institute
Carnegie Mellon University

Denial of Service Attacks

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM17-0052

Table of Contents

1 Description

This document provides a general overview of attacks in which the primary goal of the attack is to deny the victim(s) access to a particular resource. Included is information that may help you respond to such an attack.

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include

- attempts to "flood" a network, thereby preventing legitimate network traffic
- attempts to disrupt connections between two machines, thereby preventing access to a service
- attempts to prevent a particular individual from accessing a service
- attempts to disrupt service to a specific system or person

Not all service outages, even those that result from malicious activity, are necessarily denial-of-service attacks. Other types of attack may include a denial of service as a component, but the denial of service may be part of a larger attack.

Illegitimate use of resources may also result in denial of service. For example, an intruder may use your anonymous ftp area as a place to store illegal copies of commercial software, consuming disk space and generating network traffic.

2 Impact

Denial-of-service attacks can essentially disable your computer or your network. Depending on the nature of your enterprise, this can effectively disable your organization.

Some denial-of-service attacks can be executed with limited resources against a large, sophisticated site. This type of attack is sometimes called an "asymmetric attack." For example, an attacker with an old PC and a slow modem may be able to disable much faster and more sophisticated machines or networks.

3 Modes of Attack

Denial-of-service attacks come in a variety of forms and aim at a variety of services. There are three basic types of attack:

- consumption of scarce, limited, or non-renewable resources
- destruction or alteration of configuration information
- physical destruction or alteration of network components

Consumption of Scarce Resources

Computers and networks need certain things to operate: network bandwidth, memory and disk space, CPU time, data structures, access to other computers and networks, and certain environmental resources such as power, cool air, or even water.

Network Connectivity

Denial-of-service attacks are most frequently executed against network connectivity. The goal is to prevent hosts or networks from communicating on the network. An example of this type of attack is the "SYN flood" attack described in http://www.cert.org/advisories/CA-1996-21.html.

In this type of attack, the attacker begins the process of establishing a connection to the victim machine, but does it in such a way as to prevent the ultimate completion of the connection. In the meantime, the victim machine has reserved one of a limited number of data structures required to complete the impending connection. The result is that legitimate connections are denied while the victim machine is waiting to complete bogus "half-open" connections.

You should note that this type of attack does not depend on the attacker being able to consume your network bandwidth. In this case, the intruder is consuming kernel data structures involved in establishing a network connection. The implication is that an intruder can execute this attack from a dial-up connection against a machine on a very fast network. (This is a good example of an asymmetric attack.)

Using Your Own Resources Against You

An intruder can also use your own resources against you in unexpected ways. One example is described in http://www.cert.org/advisories/CA-1996-01.html.

In this attack, the intruder uses forged UDP packets to connect the echo service on one machine to the chargen service on another machine. The result is that the two services consume all available network bandwidth between them. Thus, the network connectivity for all machines on the same networks as either of the targeted machines may be affected.

Bandwidth Consumption

An intruder may also be able to consume all the available bandwidth on your network by generating a large number of packets directed to your network. Typically, these packets are ICMP ECHO packets, but in principle they may be anything. Further, the intruder need not be operating from a single machine; he may be able to coordinate or co-opt several machines on different networks to achieve the same effect.

Consumption of Other Resources

In addition to network bandwidth, intruders may be able to consume other resources that your systems need in order to operate. For example, in many systems, a limited number of data structures are available to hold process information (process identifiers, process table entries, process slots, etc.). An intruder may be able to consume these data structures by writing a simple program or script that does nothing but repeatedly create copies of itself. Many modern operating systems have quota facilities to protect against this problem, but not all do. Further, even if the process table is not filled, the CPU may be consumed by a large number of processes and the associated time spent switching between processes. Consult your operating system vendor or operating system manuals for details on available quota facilities for your system.

An intruder may also attempt to consume disk space in other ways, including

- generating excessive numbers of mail messages. For more information, please see http://www.cert.org/tech_tips/email_bombing_spamming.html
- intentionally generating errors that must be logged
- placing files in anonymous ftp areas or network shares, For information on proper configuration for anonymous ftp, please see http://www.cert.org/tech_tips/anonymous_ftp_config.html

In general, anything that allows data to be written to disk can be used to execute a denial-of-service attack if there are no bounds on the amount of data that can be written.

Also, many sites have schemes in place to "lockout" an account after a certain number of failed login attempts. A typical set up locks out an account after 3 or 5 failed login attempts. An intruder may be able to use this scheme to prevent legitimate users from logging in. In some cases, even the privileged accounts, such as root or administrator, may be subject to this type of attack. Be sure you have a method to gain access to the systems under emergency circumstances. Consult your operating system vendor or your operating systems manual for details on lockout facilities and emergency entry procedures.

An intruder may be able to cause your systems to crash or become unstable by sending unexpected data over the network. An example of such an attack is described in http://www.cert.org/advisories/CA-1996-26.html.

If your systems are experiencing frequent crashes with no apparent cause, it could be the result of this type of attack.

There are other things that may be vulnerable to denial of service that you may wish to monitor. These include

- printers
- tape devices
- network connections
- other limited resources important to the operation of your organization

Destruction or Alteration of Configuration Information

An improperly configured computer may not perform well or may not operate at all. An intruder may be able to alter or destroy configuration information that prevents you from using your computer or network.

For example, if an intruder can change the routing information in your routers, your network may be disabled. If an intruder is able to modify the registry on a Windows NT machine, certain functions may be unavailable.

For information on configuring UNIX machines, see
http://www.cert.org/tech_tips/unix_configuration_guidelines.html

For information on configuring Microsoft Windows NT machines, please see
http://www.microsoft.com/security/

Physical Destruction or Alteration of Network Components

The primary concern with this type of attack is physical security. You should guard against unauthorized access to computers, routers, network wiring closets, network backbone segments, power and cooling stations, and any other critical components of your network.

Physical security is a prime component in guarding against many types of attacks in addition to denial of service. For information on securing the physical components of your network, we encourage you to consult local or national law enforcement agencies or private security companies.

4 Prevention and Response

Denial-of-service attacks can result in significant loss of time and money for many organizations. We strongly encourage sites to consider the extent to which their organization could afford a significant service outage and to take steps commensurate with the risk.

We encourage you to consider the following options with respect to your needs:

- Implement router filters as described in Appendix A of CA-96.21.tcp_syn_flooding, referenced above. This will lessen your exposure to certain denial-of-service attacks. Additionally, it will aid in preventing users on your network from effectively launching certain denial-of-service attacks.
- If they are available for your system, install patches to guard against TCP SYN flooding as described in CA-96.21.tcp_syn_flooding, referenced above. This will substantially reduce your exposure to these attacks but may not eliminate the risk entirely.
- Disable any unused or unneeded network services. This can limit the ability of an intruder to take advantage of those services to execute a denial-of-service attack.
- Enable quota systems on your operating system if they are available. For example, if your operating system supports disk quotas, enable them for all accounts, especially accounts that operate network services. In addition, if your operating system supports partitions or volumes (i.e., separately mounted file systems with independent attributes) consider partitioning your file system so as to separate critical functions from other activity.
- Observe your system performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, CPU usage, or network traffic.
- Routinely examine your physical security with respect to your current needs. Consider servers, routers, unattended terminals, network access points, wiring closets, environmental systems such as air and power, and other components of your system.
- Use Tripwire or a similar tool to detect changes in configuration information or other files.
- Invest in and maintain "hot spares" - machines that can be placed into service quickly in the event that a similar machine is disabled.
- Invest in redundant and fault-tolerant network configurations.
- Establish and maintain regular backup schedules and policies, particularly for important configuration information.
- Establish and maintain appropriate password policies, especially access to highly privileged accounts such as UNIX root or Microsoft Windows NT Administrator.

Many organizations can suffer financial loss as a result of a denial-of-service attack and may wish to pursue criminal or civil charges against the intruder. For legal advice, we recommend that you consult with your legal counsel and law enforcement.

U.S. sites interested in an investigation of a denial-of-service attack can contact their local FBI field office for guidance and information. For contact information for your local FBI field office, please consult your local telephone directory or see the FBI's contact information web page: http://www.fbi.gov/contactus.htm

Non-U.S. sites may want to discuss the activity with their local law enforcement agency to determine the appropriate steps that should be taken with regard to pursuing an investigation.

If you are interested in determining the source of certain types of denial-of-service attack, it may require the cooperation of your network service provider and the administration of the networks involved. Tracking an intruder this way may not always be possible. If you are interested in trying do to so, contact your service provider directly. The CERT(*) Coordination Center is not able to provide this type of assistance. We do encourage you to report your experiences, however. This helps us understand the nature and scope of security incidents on the Internet, and we may be able to relate your report to other activity that has been reported to us.