Overview of Scans and DDoS Attacks
Executive Summary

The recently reported "DDoS scan" activity (http://www.nipc.gov/warnings/advisories/2001/01-009.htm and http://www.nipc.gov/warnings/alerts/2001/01-010.htm) has heightened the awareness of prudent public and private sector enterprises to the possibility of an actual distributed denial of service attack (DDoS). While NIPC has no evidence of specific intent by anyone to launch such an attack, it would be simply good business practice to take this opportunity to review existing plans and procedures that would be used if such an attack occurs. This NIPC document provides a framework for that review.

- What exactly is a DDoS attack and how do you know if you are a victim?
- What would you do if you were the target of a DDoS attack?
- What would you do if your network was being used as an unwitting accomplice to such an attack?

Denial of Service Attacks Demystified

Your enterprise network exists to provide services to your organization and to your customers. These services often take the form of transactions into and out of your network. Denial of Service (DoS) attacks interrupt that service by flooding your network or system(s) with unwanted traffic. Service is denied either because your network or system(s) are overwhelmed or because you must take your network or system(s) offline. Figure 1 depicts the scheme of a simple DOS attack. The services will be denied until the source of the attack can be identified and "calls" from that source can be "blocked."

DoS attack
Figure 1

DDoS attack
Figure 2

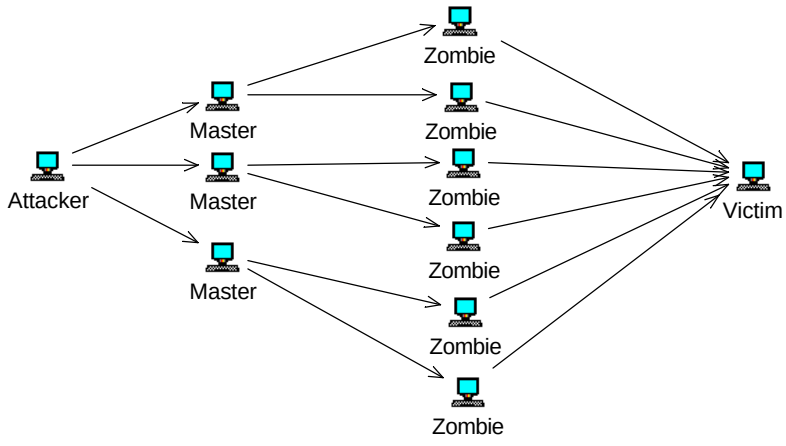

Figure 2 depicts a DDoS network where the attacker controls one or more masters which then can control several more zombies. This in turn means more pathways that need to be blocked, along with a dramatic increase in the amount of resources being consumed by the target.

In this case the attacker gains access to many different computers and sets each up to launch an independent DOS attack on command. Notice that, unlike the simple DOS attack, the DDoS attacker takes control of many computers, which then become the sources ("zombies") for the actual attack. Since the scanning activity reported by NIPC is precisely what an attacker would do to prepare for a DDoS attack, it is only prudent to review your enterprise procedures for dealing with such attacks.

How to Detect a DDoS Attack

If your company or network experiences a DDoS attack you may notice the following indicators:

- A degradation of services on the network.
- Locked up accounts due to failed attempts to access certain services.
- Inability to access services over the Internet, often illustrated by "HTTP Error 404", when a page cannot be found, although in this case it is due to a server that is too overwhelmed to respond to your request, or network unable to pass request.

For additional information on this topic, please refer to:
http://www.sans.org/infosecFAQ/securitybasics/dos.htm

What to Do If You are the Target of a DDoS Attack

If you believe that your company or network is suffering a DDoS attack you should consider going through the steps provided by the following CERT/CC analysis:
http://www.cert.org/security-improvement/practices/p082.html

The best defense in this situation often is to work with your Internet Service Provider (ISP) to ensure that it applies the necessary filters on its end, along with any firewalls and filters an individual company may have.

What to do if your network is being used for a DDoS Attack

If you believe that your company or network is being used as a "zombie" in a DDoS attack you should go through the following steps discussed in the following CERT/CC analysis:
http://www.cert.org/security-improvement/practices/p082.html

Additionally, it is important to understand that if you have machines that are being used as zombies, your network has most likely had a serious compromise, which also must be dealt with. You may need to check the rest of your network to ensure that integrity of your system remains intact.

After the Storm

Like any big storm, a DDoS attack will subside when the targets and zombies take appropriate action. In fact, the threat of a DDoS attack is often more damaging than the attack itself. It is important to keep perspective on any potential attack and take the proper precautions.

Ironically, the zombies in a DDoS attack are left with more enduring problems than the targets. Unlike targets, zombies by their very nature are systems that have been very seriously compromised. Because of this, zombie machines need to be carefully inspected to ensure that the attacker software is completely removed from the system. Unfortunately, this can often only be accomplished by reinstalling a system from a reliable backup, thereby ensuring the system's integrity, and upgrading/patching to secure the vulnerability which allowed the attacker to enter the system.

The NIPC Watch and Warning Unit can be reached at (202) 323-3204/3205/3206 or NIPC.Watch@fbi.gov