

Denial of Service, Awareness is Key

-From Department of Navy Information Assurance

"Know your enemy and know yourself and you can fight a hundred battles without disaster."

- quote from Sun Tzu's "Art of War"

For you to properly defend yourself against "Denial-of-Service Threats", you must be aware of them. Increasing your personal awareness is an integral part of prevention, and perhaps the single most important element of effective INFOSEC countermeasures. An awareness of the reality of Internet Warfare, as well as an awareness of your environment, are the keys to your Organization's computer security. Being aware does not have to involve paranoia. We can't live our lives in the shadows, but we can train ourselves to be more alert, and adjust our level of awareness as needed. For instance, if you have a good firewall and actively administer the systems on your Network, you shouldn't have to be constantly on guard. On the other hand, if your connected to the Internet without any INFOSEC measures in place, then paranoia is a good thing. Just using good common sense and remembering to pay attention to detail, and you will go a long way towards keeping you and your systems safe, in an increasingly hostile environment.

Common Threats:

- E-Mail Bombs
- List Linking
- Denial-of-Service (In General)

E-Mail Bombs

Simple and effective, these tools do nothing more than send the same e-mail message to the targeted mail host repeatedly. You might say "No big deal, just delete it" but what if you pay for exceeding a certain number of e-mails or worse yet, have those e-mails create a Denial-of-Service by overloading the mail server and bringing to it's knees. How long would your business last without e-mail? Many utilities are available on every platform to initiate this type of attack.

Countermeasure: Have your Postmaster or System administrator place the mailer identity in a Kill file or an exclusionary scheme. This will tell the server to not accept e-mail from these addresses. Most e-mail packages currently have this capability.

List Linking

Increasing in popularity, this technique yields the same result as an e-mail bomb but is accomplished differently. Basically, the Target is enrolled in as many e-mail lists as possible (of the 1000's possible). Some lists' can generate an abundance of e-mail in one day.

Countermeasure: There is no quick cure to this attack. If you desire to keep your current e-mail address, you will have to unsubscribe from each of these lists. If it is too much of a bother, ask your System Administrator or PostMaster for assistance.

Denial-of-Service (In General)

Multi-user, multi-tasking operating systems are subject to "denial of service" attacks where one user can render the system unusable for legitimate users by "hogging" a resource or damaging or destroying resources so that they cannot be used. Denial of service attacks may be caused deliberately or accidentally. Taking precautions to prevent a system against unintentional denial of service attacks will help to prevent intentional denial of service attacks. Systems on a network are vulnerable to overload and destructive attacks as well as other types of intentional or unintentional denial of service attacks. Three common forms of network denial of service attacks are service overloading, message flooding, and signal grounding. It is important for system administrators to protect against denial of service threats without denying access to legitimate users.

Countermeasure: In general, denial of service attacks are hard to prevent. Many denial of service attacks can be hindered by restricting access to critical accounts, resources, and files, and protecting them from unauthorized users. Making sure you stay up on Operating System patches is your best defense.