Resisting against DoS attacks

Denial of Service - Denial of service attacks is simply a way of making ordinary visitors on a website unable to access the website. If configured correctly, an IIS service can really protect you from basic network attacks.

Have you ever been exhausted from a company and wanted revenge? Have you ever been fired and felt they were unfair? When you were young, did you smash a basketball into someone's mailbox while you borrowed your car?

We are all human beings. At some point we may be angry and try to vent our anger. The motive is sometimes revenge, jealousy, greed or even simply bored.

But we are not always the ones to vent, sometimes we are their victims. Do you do something wrong with someone? Sometimes they are turned into victims for no reason at all. For example, you are running a website with a high profile level. That is an opportunity for all attackers. The motive is not missing, it can be anything that makes them uncomfortable. You must always maintain the website 24 hours a day and 7 days a week. At that time, you have to prepare some effective preventive measures yourself before trying to figure out the type of attack that destroys your website.

Source: ***information-age*** Saying that, but in return, there are three main types of server attacks: intentional destruction, theft or denial of service. This article will show you the most basic knowledge about Denial of Service (DoS) and how to use IIS service to combat it. To the limit, we only want to stop at IIS and have not discussed other areas such as router configuration or DNS hijacking temporarily.

If configured correctly, an IIS service can really protect you from basic network attacks. Usually combined with general security procedures, you can protect your server against most of these attacks.

What is the Denial of Service?

Denial of Service - Denial of service attacks is simply a way of making ordinary visitors on a website unable to access the website. This way can be done in a way that takes up 100% bandwidth, 100% CPU, 100% RAM, fills the hard drive, destroys the kernel or server applications, redirecting traffic so that users never access to the website you want to use. A few years ago, a number of vulnerabilities were discovered in Windows NT and the IIS service. There are also some weaknesses in the TCP / IP protocol that could be exploited to attack DoS from a website. We will not mention how an attack works but mainly emphasize the method that can be used to protect your computer against any attack.

Update the patch

Keeping track of many common security programs, you can give yourself plenty of experience to protect yourself against attacks. The most basic measure is to always update the latest manufacturer's issues and patches. Most important is the Microsoft security bulletin for Windows NT and IIS. You should also regularly monitor mailing lists and secure websites to deal with other current security issues.

One drawback of this method is that you may be introduced to codes that are not carefully tested, and may become the cause of problems for your server. Patches should be carefully analyzed and backed up before applying them.

"Closed" unnecessary services

Server software applications and services will have more errors when running at the same time. Turn off all services that do not have a clear use on your website. If you do not need the FTP anonymous protocol, disable it until necessary. Similar to Terminal Server, NetBIOS, Telnet and Mail servers. If you want the web server to work, remove everything except the special programs that are used to run and administer the server.

Same for ISAPI extension mapping and sample applications on IIS. Get rid of any unnecessary extension mappings to use the brightest web root.

Maintenance

Upgrade the scheduling and disk deletion services so that the temp folders and package in your device have plenty of storage space. You should also regularly monitor log size and package files spread across multiple volumes or drives if possible.

Block network services

The most basic advice to protect the security and amount of time of a web server is to remove the NetBIOS protocol. There are several types of attacks targeting NetBIOS and the best solution is to completely exclude it from the web server. Other protocols and clients (such as Client for Microsoft Networks) should be carefully considered when allowing them to operate on a web server.

When configuring the network adapter, you should set up your own IP address, network port, and DNS service yourself instead of leaving the default. Because it is very vulnerable to exploiting DHCP vulnerabilities.

Although it rarely works, use TCP / IP filters on the server. You should only allow ports to use as 80, 443 or 21 for FTP services. If provided on the right limit, you can also use a third-party firewall application.

Here are some registry settings that can be used for IIS service references:

Registry key REG_DWORD **Value Type** 2
HKLMSYSTEMCurrentControlSetServicesTcpipParametersEnablePMTUDiscovery
HKLMSYSTEMCurrentControlSetServicesTcpipParametersSynAttackProtect
HCLMSYSTEMCurrentControlSetServicesTcpipParametersNoNameReleaseOnDemand REG_DWORD
REG_DWORD 0 1 HCLMSYSTEMCurrentControlSetServicesTcpipParametersEnableDeadGWDetect
HCLMSYSTEMCurrentControlSetServicesTcpipParametersKeepAliveTime REG_DWORD REG_DWORD 0
300,000 0 HCLMSYSTEMCurrentControlSetServicesTcpipParametersEnableICMPRedirects

HCLMSYSTEMCurrentControlSetServicesTcpipParametersPerformRouterDiscovery REG_DWORD REG_DWORD 0
If these settings do not prevent attacks, it is better to control over TCP / IP parameters. Look in the resource sets for more details on all related settings.

Use the Performance Counters and Alerts component .

Learning how to use Windows 2000's Performance Counters and Alerts component can provide you with effective measures against DoS attacks. That is, some executable counters can intelligently indicate a DoS attack. For example, counters that monitor microprocessor data, RAM, hard disk, TCP or ICMP can provide insight into the existence of the server. By adding warnings to limit ahead, you can be sure that you will get some correct warnings in case of an attack.

Now, if someone is planning to break your website, with some precautions, you are completely in control when they come. Most of these techniques are very simple, but must be done regularly. At the very least, you can know how the security world is happening and actively deal with those who want to sabotage you.