

Withstanding Denial of Service Attacks

Mark Burnett 2000-06-27

Have you ever been ripped off by a company and wanted to get revenge somehow? Have you ever been terminated from a job and felt you were treated unfairly? As a teenager did you ever take a baseball bat to someone else's mailbox while speeding by in a friend's car?

We are all human and at some point we are angry with someone somewhere. Sometimes we just take out our anger on the next person who passes by. Our motivations could be revenge, jealousy, greed, or even just boredom.

But sometimes we are the victims of someone else's anger. Maybe we have wronged someone or maybe we are just a random victim. If you operate a high-profile web site, chances are that someone sometime will try to take you down. Their motivations may vary but whatever they are, you must still keep your site going 24 hours a day, seven days a week.

There are three basic ways in which a server can be attacked. It can be vandalized, robbed, or denied service. This article will be covering denial of service (DoS) and what can be done to make an IIS server more resistant to DoS attacks. This article will deal specifically with IIS and not cover other areas such as router configuration or DNS hijacking.

Configured correctly, an IIS server can actually be quite resilient to network-based attacks. Often, by following common security procedures, one can protect a server from the majority of these attacks.

What is Denial of Service?

Denial of Service is simply making a web site inaccessible to a site's normal visitors. This can be accomplished a number of ways including 100% bandwidth utilization, 100% CPU utilization, 100% RAM utilization, filling a hard drive, crashing the kernel or server applications, or redirecting traffic so that it never reaches the intended site. In the last few years there have been a number of vulnerabilities discovered in Windows NT and IIS that result in many of those conditions. There are also a number of weaknesses in the TCP/IP protocol that can be exploited to deny service from a web site. We will not be covering here the specifics of how each attack works but rather what methods can be used to protect from any number of attacks.

Keeping Patched

By following many common sense security procedures you can take a big step towards helping your site stand its ground under attack. The most obvious of these procedures is to keep up-to-date on the most current issues and vendor patches. Most importantly are Microsoft's [security bulletins](#) for Windows NT and IIS. You should also frequently monitor mailing lists and security web sites for other current security issues.

One downside of keeping up-to-date on patches is that you may be introducing code that has not been fully regression tested and may cause problems with your particular server. Patches should be analyzed carefully and backups should be made before applying them.

Closing Doors

Server software applications and services do have bugs and when you have more services running, you increase the number of battle fronts that must be monitored. Shut off all services that do not have a specific purpose for your web site. If you do not need anonymous FTP, disable it until the occasion rises that you do. The same is true for Terminal Server, NetBIOS, Telnet, and Mail servers. If you want a web server to keep serving, remove everything except that which you specifically are using to run and administer the server.

The same is true for ISAPI extension mappings and sample applications on IIS. Remove every extension mapping that you do not specifically use and [keep your web root clean](#).

Regular Maintenance

Take advantage of the scheduler service and the disk cleanup utility to keep your temp directory and swap volumes clean with plenty of extra drive space. You should also regularly monitor log sizes and spread swap files across several volumes or drives if available.

Lock Down Network Services

The most basic advice one can give to protect the security and uptime to a web server is to remove the NetBIOS protocol. There are a number of attacks targeted at NetBIOS and the best solution is to eliminate it completely from a web server. Other protocols and clients (such as Client for Microsoft Networks) should be carefully considered when enabling them on a web server.

While on the network adaptor configuration, it may be a good idea to manually configure the IP address, gateway, and DNS servers to protect from attacks that exploit weaknesses in DHCP.

Although rarely done, enabling TCP/IP filtering on the server can also be a great protection form a number of attacks. You should only enable the ports that you will specifically be using such as 80, 443, and possibly 21 for FTP services. Keep in mind, however, that any TCP/IP filtering restrictions you set will apply to all adaptors on the system. If that proves to be too restrictive, the you should then consider a third-party firewall application.

There are a number of registry settings that can be used to make IIS more resistant to attacks based on TCP/IP protocol flaws, such as SYN floods. The recommended settings for these registry keys are as follows:

Registry Key	Type	Value
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect	REG_DWORD	2
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery	REG_DWORD	0
HCLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\NoNameReleaseOnDemand	REG_DWORD	1
HCLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect	REG_DWORD	0
HCLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime	REG_DWORD	300,000
HCLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery	REG_DWORD	0
HCLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirects	REG_DWORD	0

If these settings do not stop an attack, finer control can be gained over the TCP/IP parameters. Refer to the resource kits for more detailed descriptions of all the relevant settings.

Use Performance Counters and Alerts

Learning to use Windows 2000's Performance Counters and Alerts can prove to be very effective in protecting against DoS attacks. There are a number of performance counters that can be excellent indicators of a DoS attack. For example, counters that monitor the processor, RAM, hard disk, TCP, or ICMP data can all provide a good insight into how well your server is surviving. By adding alerts to predefined warning levels, you can be sure that you will have some warning in case of an attack.

Eventually someone will have some motivation for taking down your website. By taking these few precautions you can be ready when they come. Most of these techniques are very simple to implement but do require taking regular time each day to know what is going in the security world and stopping those who would like to knock your site to its knees.

Relevant Links

[Latest Microsoft Security Bulletins](#)

Microsoft

[Locking Down NT](#)

SecurityFocus

[Locking Down IIS](#)

SecurityFocus

[Privacy Statement](#)

Copyright 2006, SecurityFocus