Steven.Thode

From: CramSession [listboss@list.cramsession.com]
Sent: Wednesday, November 28, 2001 7:17 PM
To: Steven.Thode
Subject: Security Essentials: Hardening TCP/IP Stacks

Win2K Insider
38,000 Subscribers Worldwide
November 28, 2001
Issue #69
CramSession StudyGuides InfoCenter Discussions SkillDrill Newsletters CramSession

Feature

Hardening TCP/IP Stacks on Internet-Connected Machines Read it

Ask Uncle Bill

Q and A's Read it

Security Advisories

No New Security Advisories This Week!

News Headlines & Resources

Windows 2000 Security Hotfix Tools Read it
Windows .Net Server Beta 3 Details Read it
A Winipcfg Knock-off Available for Win2k/NT/XP Systems Read it
Best Of The "I Passed 70-240" Posts Read it
Windows XP in Small Peer-to-Peer Networks Read it
Windows XP Admin Tools Beta for Windows 2000/.Net Server Read it
Expand Screen Real Estate with WinXP Multiple Monitors Read it
How to Enable ISA Server to Log to an Oracle Server Read it
Support Webcast: Using the Microsoft Security Tool Kit Read it

Download of the Week

Proxy Log Analyzer 1.06 Read it

Feature

Hardening TCP/IP Stacks on Internet-Connected Machines

to top

Have you looked at the packet filter logs on your Windows 2000 machines that are directly connected to the Internet? It can turn you into an absolute paranoid! Why are all these people scanning your computer? Because they're looking for weaknesses that they can exploit.

In the good old days, hackers were only interested in the "big fish". These big fish were high profile Web sites and corporate or government servers. These were real hackers and crackers that enjoyed the challenge of breaking into sites just to see if they could. The clever hackers of yore are now far outnumbered by legions of AOL script kiddies connected to broadband networks. With their predefined scripts and GUI interfaces, it's a no-brainer California Youth Authority wash-out to take down your precious Web servers.

Denial of Service Attacks

Some of the most problematic attacks that can be launched against your box are Denial of Service attacks. Denial of Service (DoS) attacks are network-based exploits aimed at making a computer, or particular services on a computer, unavailable to legitimate network users. It's difficult to defend yourself against DoS attacks.

The best thing you can do to prevent DoS attacks from cratering your server is to keep your systems updated with the latest security fixes. These fixes can always be found at www.microsoft.com/security. Pay special attention to the IIS fixes as it's almost always Web services that will make your Internet-connected box vulnerable.

Another thing you can do to prevent DoS attacks on your Windows 2000 Pro and Server computers is to harden the TCP/IP protocol stack. The default TCP/IP stack configuration is tuned to handle normal intranet traffic. Normal intranet traffic is assumed to be friendly and not dedicated to bringing your business down. You'll have to decide if your network fits that description. Nevertheless, when a machine is directly connected to the Internet, you should consider hardening the TCP/IP stack against DoS attacks.

Using the Registry to Harden the TCP/IP Protocol Stack

The following is a list of TCP/IP-related Registry Values that can be configured to harden the TCP/IP stack on machines directly connected to the Internet. All these values are found under this Registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

Just click Run and type regedt32 in the Open text box. That will open the Registry Editor where you can make the appropriate changes.

Registry Values Used to Harden the TCP/IP Protocol Stack

SynAttackProtect

Key: Tcpip\Parameters
Value Type: REG_DWORD
Valid Range: 0,1,2
Default: 0

This registry value causes TCP to adjust retransmission of SYN-ACKS to cause connection responses to time out more quickly in the event of a SYN Attack.

Parameters:

0:
Default Value - Normal protection against SYN Attacks.

1:
This setting provides better protection. This parameter causes TCP to adjust the retransmission of SYN-ACKS to cause connection responses to time out more quickly if there is a SYN-ATTACK in progress. This determination is based on the TcpMaxPortsExhausted, TCPMaxHalfOpen, and TCPMaxHalfOpenRetried.

2:
This setting provides the best protection. This value configures additional delays to connections to quickly timeout TCP connection requests when there is a SYN Attack. I recommend this setting. Note that the following socket options will no longer work on any socket when the value is set to 2: Scalable windows, and per adapter configured TCP parameters such as for Initial RTT, window size.

EnableDeadGWDetect

Key: Tcpip\Parameters
Value Type: REG_DWORD
Valid Range: 0, 1 (False, True)
Default: 1 (True)

TCP is allowed to perform dead-gateway detection when this parameter is set to 1. When dead-gateway detection is enabled, TCP can change to a backup gateway. Backup gateways are defined in the Advanced section of the TCP/IP configuration dialog box found in the Network Control Panel.

Set this value to 0. An attack could force the server to switch gateways and cause it to switch to an unintended gateway. Well, at least unintended by YOU.

EnablePMTUDiscovery

Key: Tcpip\Parameters
Value Type: REG_DWORD
Valid Range: 0, 1 (False, True)
Default: 1 (True)

TCP will attempt to discover the Maximum Transmission Unit (MTU or largest packet size) over the path to a remote host when this value is set to 1. The Path MTU discovery allows TCP to eliminate fragmentation at routers along the path that connects networks with different MTUs. Fragmentation adversely affects TCP throughput. When you set this

parameter to 0, an MTU of 576 bytes is used for all connections that are not to hosts on the local, directly connected, subnet.

Set this value to 0. An attacker could force MTU to a very small value and over-work the stack which will essentially make useful network connections to the server impossible.

KeepAliveTime

Key: Tcpip\Parameters
Value Type: REG_DWORD-Time in milliseconds
Valid Range: 1-0xFFFFFFFF
Default: 7,200,000 (two hours)

This value controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet. If the remote system is still reachable, it acknowledges the keep-alive packet. Keep-alive packets are not sent by default. This feature may be enabled on a connection by an application. The recommended value is 300,000 (5 minutes).

NoNameReleaseOnDemand

Key: Netbt\Parameters
Value Type: REG_DWORD
Valid Range: 0, 1 (False, True)
Default: 0 (False)

This value determines whether the computer releases its NetBIOS name when it receives a name-release request. It was added to allow the administrator to protect the computer against malicious name-release attacks. The recommended value is 1 (true).

PerformRouterDiscovery

Key: Tcpip\Parameters\Interfaces\
Value Type: REG_DWORD
Valid Range:
0: Disabled
1: Enabled
2: Off by default, DHCP-controlled
Default: 2

This value controls whether Windows 2000 attempts to perform router discovery on a per-interface basis. The recommended value is 0. This will prevent bogus router advertisements. Use the value in Tcpip\Parameters\Adapters to figure out which value under the Interfaces key matches the network adapter.

Summary

There is a lot you can do to protect the box you have directly connected to the Internet. Keep your eyes peeled for the latest security fixes and harden your TCP/IP stack. Even though DoS attacks are tough to protect yourself against, if you take just a few steps you can protect yourself from most of the known attacks.

This week's feature article by
Thomas W. Shinder,
M.D., MCSE

Ask Uncle Bill

to top

Q and A's

Question:

Hi Uncle Bill:
Do you have any suggestions on how to upgrade a motherboard and processors on a Win2K machine without reinstalling all the applications? I heard that Win2K backup could do the job. I hate to reinstall cause a lot of the applications are older and many have been gotten via the web and are no longer available. Want to upgrade my dual cpu's from 600 to 1.2 and get a new motherboard to accommodate them.
--llpick

Uncle Bill says:

We found ourselves in the same position at one time. All we did was take the disks and put them the same IDE positions in the new computer. The big difference is that we went from Uniprocessor to Uniprocessor machine. Plug and play was able to handle all the new hardware on the new box. You might have to upgrade to the multiprocessor kernel after moving the disks to the new box.

Question:

Uncle Bill:
How many monitors can I connect to my Windows XP Professional computer? Some people say 9 and some people say 10. Thanks!
--MultiMon

Uncle Bill says:

You can connect up to 10 monitors to a Windows XP Professional computer. If you use XP Home, then you're limited to 2 monitors. Watch out for radiation burns if you plan on connecting 10 monitors and putting them all on your desk facing you :)

Don't Be Shy!

Got a question about MCSE certification or an event log error that just won't go away? Send it in! We'll be answering a question or two every week. Send your submissions to Uncle Bill **here**.

Security Advisories

to top

No New Security Bulletins

Happy Holidays!
No new security bulletins from Microsoft for this week.

News Headlines and Resources

Windows 2000 Security Hotfix Tools

to top

Get on board Microsoft's Strategic Technology Protection Program by using two cool tools. The Network Security Hotfix Checker and the QChain.exe tools will get you to the secure place you want to go to.

Read more...

Windows .Net Server Beta 3 Details

to top

.Net Server Beta 3 has been released and it's got more cool toys than an after-Christmas Holiday sale! This software picks up where the Windows 2000 Server family leaves off. Check this site for some details and screen shots.

Read more...

A Winipcfg Knock-off Available For Win2k/NT/XP Systems

to top

Does the text output of the ipconfig tool scare you? Then get back to the cool 9x experience by downloading the wntipcfg tool from Microsoft. It's just like the cheesy winipcfg you know and love from your 9x systems. And, it's free!

Read more...

Best Of The "I Passed 70-240" Posts

to top

We're entering the last month of availability for the 70-240 Accelerated Exam for MCPs. If you're planning on taking this exam this month (or know someone else who is), take a moment to read the advice offered by those who have passed this 4-hour multiple-choice monster.

Read more...

Windows XP in Small Peer-to-Peer Networks

to top

Do you run or consult with "micro" business networks? These are networks with ten or fewer computers. If so, you need to bone-up on Windows XP's new peer networking capabilities. These capabilities make setting up a network like shooting fish in a barrel.

Read more...

Windows XP Admin Tools Beta for Windows 2000/.Net Server

to top

Windows XP is pretty cool, but they forgot something: an adminpak.msi that allows you to manage Windows 2000 servers. The wait is over! Here are the Administration Tools that you can install on XP machines.

Read more...

Expand Screen Real Estate with Windows XP Multiple Monitors

to top

If you live at your computer, you know that a lot more work can be done faster using multiple monitors. Windows XP expands on the Windows 2000 multimonitor support features. Deb Shinder shows you the ropes here.

Read more...

How to Enable ISA Server to Log to an Oracle Server

to top

Euticio Montelongo breaks new ground with the seminal article on how to get ISA Server to log to an Oracle database. Script code included!

Read more...

Support Webcast: Using the Microsoft Security Tool Kit

to top

In this session they will walk you through the three installations of the Security Tool Kit. They'll review the contents of the tool kit and discuss all the tools in the kit that help you stay secure.

Read more...

Download of the Week

Backup Plus

to top

The cool little share backup program makes it easy to customize your backups. It works nicely with removable media such as Zip and CDR disks. You can create timed backups and special backup configurations with just a couple of clicks. If you want to script it, there's a CLI too! This baby works nicely in Windows XP.

Read more...