The NETSTAT Command

Description: Steve and Leo describe the operation and use of the universally available "Netstat" command – available in every desktop operating system from Unix and Linux through Windows and Macs. "Netstat" allows anyone to instantly see what current Internet connections and listening ports any system has open and operating. Mastering the power of this little-known command will greatly empower any security-conscious computer user.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-049.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-049-lq.mp3

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 49 for July 20, 2006: Netstat.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com.

It's time to talk security with Steve Gibson. Hey, Steve.

Steve Gibson: Hey, Leo. Great to be back with you.

Leo: I was in Boston earlier in the week. Boy, was it hot. It's hot everywhere. It's hot today.

Steve: Oh, yeah.

Leo: It's hot.

Steve: Yeah. Well, and I don't know about Northern California, but down here in the south, I guess because of monsoon season, it is so humid.

Leo: Oh, that's unusual.

Steve: I mean, it's not dry heat, which, you know...

Leo: Oh, that's not good at all, yeah.

Steve: No, because then your own body's natural perspiration can't be really used very effectively to cool you off through evaporative cooling, so...

Leo: And we're learning something about all kinds of things in this show. So you're kind of one of them autodidacts, aren't you, where you just...

Steve: Well, I'm curious about everything, so I spend time hear and there learning what I can. But I didn't realize, I mean, and people may not, that, you know, since we're on the topic, that we are – even though we're not, like, sweating profusely, we're constantly perspiring as part of our body's temperature regulation system. And we depend upon it being dry in order for perspiration to evaporate, which creates the cooling effect. Because of course it takes energy to move water into vapor. So that reduces our temperature.

Leo: Well, I'm schwitzing right now because it's very hot out here. The reason I brought it up was I was approached by a cable guy in Texas. And he said, you know, I'm a small cable operator in Texas, and we love Security Now!, and we would just like to know if we can kind of, I don't know, send it to our customers or something so that – because it's just we want them to know this information. And I thought, bravo. And I said, absolutely, please do. You know, our license prohibits commercial usage without permission, so he was right to ask for permission. But I think you'd agree that we're just here to get that information out. And I think it's wonderful that an Internet service provider would actually give the podcast to his customers.

Steve: Oh, absolutely.

Leo: Saying, you know, listen to this, you need to know this stuff.

Steve: Yeah. And, you know, I would imagine that some percentage of them might – will hopefully get hooked and think, hey, I want to know about this stuff.

Leo: Well, it's good for us, absolutely. You know, any way we can build the audience, we're happy to do it. Although the audience numbers are out, and we're pretty much over 100,000 every show now. So that's very good news.

Steve: Very cool.

Leo: And I also wanted to mention that there's a big Windows security flaw. I sent you this link yesterday. Guess what, the WMF flaw that you've been talking about.

Steve: Well, that we talked about, you know, very controversially at the beginning of the year. That was, you know the first big news of 2006 was the Windows Metafile vulnerability that was discovered. Basically old code, for whatever reason, in Windows, that allowed images, just a

standard old image...

Leo: That's what a WMF file is, it's an image file.

Steve: Exactly, to execute code that was contained in the image. And not surprisingly there have been, you know, sort of in the background, relatively quietly, malware and malicious sites have been using this to exploit, to install trojans of various sorts in unpatched computers. What you found yesterday, Leo, was really sort of alarming because apparently the very popular MySpace domain, as well as several others, have been hosting some ads that contain and use the Windows Metafile vulnerability. And by backtracking where the ads go and what the malware was doing, some security researchers are of the opinion that more than 100 –I'm sorry, more than a million instances of this malware has been installed using this Windows Metafile vulnerability. Which, well...

Leo: That's amazing.

Steve: It's a big number. Well, but what's really puzzling is, you know, who? What million people? Because in order to – I mean, this vulnerability was fixed, as you will remember, even out of Microsoft's normal upgrade cycle because it was such a big problem. You know, and...

Leo: They patched it, you know, six months ago.

Steve: Well, and we had Ilfak on the show, you know, because he came up with a quick little fix for it in order to – because we didn't know if Microsoft was going to. So for someone to be infected by this today, they can't have updated the security on their machine all year. I mean, for seven months.

Leo: Well, now of course MySpace is huge. These were pushed out in a banner ad which was provided by a provider. So MySpace didn't push the ad or even host it. You know, as with all banner ads, they're hosted by the agency.

Steve: They were using a third party.

Leo: Right. And Webshots and a number of other sites also apparently pushed out the ad. But the point is that so many – MySpace is so huge, tens of millions of subscribers, that it was possible for them to infect a million computers.

Steve: But again, a million...

Leo: Unpatched.

Steve: ...not patched computers.

Leo: Yeah.

Steve: So, you know, certainly nobody listening to this show needs to worry because there's nobody listening to us that isn't, you know, updating their machine all the time.

Leo: And the other thing to point out is that you would get this virus not through any action on your own. And that's what really made it deadly. Just by looking at this MySpace page, if that banner ad happened to come up and you had an unpatched computer and you were using Internet Explorer, you'd be bit.

Steve: Yup.

Leo: You'd have that code. And they were putting a trojan horse code on people's computers. So, wow, a really dramatic example of what can happen if you don't follow basic security procedures.

Okay. Any other issues we want to cover before we get to our topic at hand?

Steve: I think we're ready to go.

Leo: What is the topic at hand? I didn't ask.

Steve: Network monitoring. And, you know, of course that phrase or that term has many different meanings. In this case I want to talk about a tool which is built into, well, that started back with UNIX and is in virtually every machine, whether it's a UNIX, Mac, Linux, FreeBSD, and even Windows from the beginning. It's a command called "Netstat." And the issue is, how do you know what your machine is doing; what connections it has to the Internet; what services may be open and running in your machine, wanting to accept connections; and basically sort of, like, what's going on in your machine.

Now, there's the Netstat command that I'm going to sort of focus on, and then there's a GUI-ized version that our friends at Sysinternals, Mark Russinovich, wrote. Oh, and by the way, there is a bit of news, not really wonderful news from the standpoint of the whole industry. Sysinternals is now a division of Microsoft.

Leo: Oh, no. Oh, no. Oh, and Sysinternals is – Mark Russinovich, I guess, is the frontman, but I think there's others involved, but...

Steve: Well, yeah. He and Bryce are the two main guys. And Mark is the heavy-duty coder who's written over the last ten years – Sysinternals is ten years old, was founded in 1996. And it took, you know, they grew it and built it, and it became a serious, you know, wonderful resource. We've talked about Sysinternals utilities all the time. Mark is...

Leo: They discovered the Sony rootkit, most notably, but they've done a whole lot of other great stuff.

Steve: Well, and it was RootkitRevealer that we've talked about.

Leo: Which was their program, yeah.

Steve: That's another one of Mark's pieces of freeware. I mean, Sysinternals distributes a whole bunch of freeware. Then they had their commercial side, which is Winternals, and they sell, you know, like in some cases pro versions of their freeware and stuff that they don't offer in freeware. But, I mean, just it's been a tremendous source of super utilities over the last ten years. And Microsoft decided that they wanted it all.

Leo: Well, I'm thrilled for Mark and Bryce. I hope they made a ton of money.

Steve: Yes, in fact he and I exchanged some email yesterday because I told him I wanted to talk about TCPView, which is his GUI-ized version of Netstat. But not surprisingly, the moment the announcement was made you could hardly get to their site.

Leo: Yeah, I bet.

Steve: Because everybody was saying, oh no, before it goes away I want to get everything.

Leo: And I'm sure that's not the case. I'm sure Microsoft will keep all that stuff up. I would hope.

Steve: I wouldn't be that sure. Immediately all of the EULAs changed.

Leo: Oh, dear.

Steve: And the terms began to change. Mark explained what – the reason I exchanged email a couple times with Mark yesterday was I said, you know, no one can get to your site now. I mean, it was literally – it was slashdotted, as they say, because so many people were trying to grab the latest state of the site before it went away, if it was going to. You know, and we've had things go away before that we thought would be here forever. So anyway, Mark explained that he was just in the process then of moving the site to much faster hardware and connection. And sure enough, it's now back up and running and just fine. Because I wanted to ask him whether I could redistribute TCPView. He said, "I am no longer in control of the site."

Leo: Oh, boy.

Steve: So that's no longer his responsibility. Somebody at Microsoft presumably has taken that over. I mean, he's excited. It is a – certainly I'm sure he and Bryce did really well in being acquired by Microsoft with, you know, probably huge stock trade and so forth. So...

Leo: Yeah. And, you know what, Microsoft can really use their skills and their tools. So I think it's – if it gets their stuff out to a broader audience, I'm happy about it. But we do hope that they'll continue to offer the stuff for free that they have been offering because it's so useful. And they'll continue to do the work they've been doing.

Steve: Well, also Mark has really continually been moving the code forward, adding features here and there, you know, I mean, really tending his flock of freeware.

Leo: He deserves a payday.

Steve: That will end. So, you know, it is pretty much – it's pretty clear that we're not going to continually have, you know, a forward motion of those things. I mean, I think this era is over. So for what it's worth, for people listening to the podcast who know...

Leo: [Indiscernible] now...

Steve: Yeah. Well, and all – you might just go to www.sysinternals.com and just browse around. There's OS utilities, network utilities, you know, security stuff, all kinds of good stuff. I would advise that you go sooner rather than later and just grab the things that look good to you.

Leo: I have to point out, this is one of the reasons I am a fan of open source. Had he open-sourced it and GPLed it, it wouldn't matter if he was going to continue to develop it because others would. But we're not in that position now. Microsoft owns it.

Steve: Right.

Leo: So it's, you know, that is one reason why I'm a big fan of open source utilities. The other reason is that you can look at the source and make sure they do what they say they're going to do. He releases some source, I think. But I don't think he's open-sourced any of it, so...

Steve: Correct. He has – he's sort of – what he'll do is he'll have sort of juniorized versions of his utilities in source form, just because he wants to give things away. And, you know, I mean, he was truly a benefactor to the community. And then the more fancy things would normally not be available in source. And as I said, he does also have some commercial for-pay pro versions. For example, there is a TCPView Pro that offers some additional features beyond what the free one does.

Leo: Right. Oh, well. You hit me with a shock. But you can still get TCPView. And so – and actually I've always used Netstat. I didn't realize TCPView was a GUI front end on that. So that's good to know.

Steve: Right.

Leo: Yeah.

Steve: Right. Well, and in fact it's interesting. Now, as you know, Leo, I'm becoming a little more of a Mac person recently. I've had to – I've been working with some new technology for the GRC site, wanting to do menuing, add some good navigation and menuing to GRC.com which, you know, it sorely needs. And I wanted to make sure that it would run under Safari and

the older IE 5.2 over on the Mac. So I've been over on the Mac. And I thought, you know, I ought to make sure that the stuff I'm going to talk about today, if there are issues for, like, the Netstat command on the Mac, that I talk about that. So I'm adding a little more Mac support to my repertoire.

Leo: Right. Good. Well, thank goodness somebody gave you a MacBook.

Steve: Yeah, the neat guys at Nerds On Site, they wanted me to participate in their conference at the end of this month via iChat, so they provided me with a MacBook so that I could do that.

Leo: They've done more good than they could know. The Mac community thanks them. So Netstat, well, and there is an analog to Netstat, in fact I think it's called Netstat, in UNIX and on the Macintosh, is there not?

Steve: Oh, it started there. I mean, it was Netstat on UNIX. The idea is – okay, so let's rewind things a little bit here. You've got a computer. We've talked many times about how there's a NIC, a network interface card, a network adapter which is connecting you physically to the 'Net. Then we've talked about this, the so-called TCP/IP stack, this essentially a stack of layers – that's why it's called a stack – of technology that interfaces the low-level Internet raw data to the operating system. Well, and we've talked about the UDP protocol and TCP and the notion of listening ports and ports being open and connections being established, you know, and SYN packets and ACKs and all that.

Well, the Netstat command, which originated with all of this technology, which originated in UNIX and was then moved over into Windows and other UNIX-like operating systems, it's the network status command that allows you to find out what's going on. Now, for that reason it's really useful. There's really nothing else that does this. And that's why I wanted to give it its own episode of Security Now!, to talk about the Netstat command and to introduce it to people, to invite people – this is the kind of thing you're probably going to want to listen to this podcast again. Maybe if you're listening to it in your car while you're commuting, you're going to want to, you know, rewind it, listen to it again sitting in front of your computer and poking at this as I talk about what this command does and how useful it is. Because it allows you to know exactly what's going on with this lower level networking in real-time in your computer. This is the way...

Leo: I'll tell you what. I'll run the UNIX version on my Mac, and everybody else run the Windows version, and I'll tell you if there's any differences on here.

Steve: Well, and for that reason over on UNIX you want to fire up your terminal application.

Leo: I've got it up here, yup.

Steve: And in UNIX the so-called "sockets," which is the term that UNIX originated, over in UNIX it's used much more extensively than it is in Windows. There are some things called "domain sockets." And if you just do the Netstat command on a Mac, you'll see...

Leo: Oh, boy.

Steve: ...way more stuff, yes, than you want. So what you need to do on a Mac is you need – there's an F command line option. So you'd say netstat, space, then dash, F-I-N-E-T [netstat –finet]. You can put a space between the F and the INET if you want to. INET's short for Internet. So if you do netstat, then space, dash F-I-N-E-T, that says only show the Internet socket activity, not the whole UNIX – don't include the UNIX sockets, which is not stuff that we really have any interest in at all.

Leo: Right.

Steve: So everything that I'm talking about – well, and also I should say that the command lines – I'm going to focus on the Windows side because we have a, you know, a huge...

Leo: That's where most of our listeners are, yeah.

Steve: It's where most of our listeners are. Also over on the Mac, if you have the terminal window open, you can say man space netstat. M-A-N, short for manual, man space netstat [man netstat], that'll give you a screen of – basically that will help you translate the things I'm talking about specifically over into the UNIX side. And of course this works for FreeBSD and Linux listeners...

Leo: As well as Mac, yup.

Steve: ...also, right.

Leo: All right. So we'll do the Windows version here.

Steve: Yes.

Leo: Now, first of all, you've got to get your command line up by clicking Start, entering Run, and typing "netstat." Or actually type command, I'm sorry, CMD, and then you'll have a command line window, so you can do...

Steve: Either that or, in Windows users, all Windows systems start out with an option under the start menu that says MS-DOS Prompt. And so probably the easiest thing for people to do is just hit Start, go to Programs – I think it's under Accessories.

Leo: I don't have that. You have that? MS-DOS Start, really? Oh, yeah.

Steve: No, no, MS-DOS Prompt.

Leo: I have Command Prompt because it isn't MS-DOS in XP.

Steve: Or Command Prompt.

Leo: Right, right, right.

Steve: Yeah. They've also changed the name from time to time.

Leo: There's no MS-DOS anymore, that's why.

Steve: And so that will bring up a window. Now, you want to start off also with sizing this correctly. Sometimes the window is sizable, in which case you want to probably stretch it out so it's the full height of your screen. When you are doing these things with Netstat, depending upon how much network activity you have, Netstat will be doing sort of a log of everything happening on your machine, which can get long.

So the first thing you want to do is to stretch the window out. But you may want to be able to scroll back further if this window scrolls a lot. So the way you can do that is click on the little icon in Windows on the upper left-hand side of the window, and then choose Properties. Then there's a tab there, the Layout tab, shows both a screen buffer and a window size. If you change your screen buffer – this is in the number of lines – change that to maybe, I mean, it can be big. Set it to 1,000 while you're doing this. That way you'll be able to scroll way back as far as you need to if the stuff we're doing scrolls off the window. So that will allow you now – so basically you've got now a command window opened which allows you to enter commands. And we've got the window, you know, so that it's tall on your screen. And if you set your screen buffer size to, like, 1,000, and then clicked okay a few times to make it happy, you should now be able to scroll way back into the past.

Leo: Yes.

Steve: For people who haven't used this command window a lot before, you want to know how to clear it in order to – from time to time, like before you issue a command, you might want to just get rid of all of the history that has scrolled by. The command for that is CLS. That's the clear screen command. So CLS, and then press Enter, will wipe that window clean and get ready for your next command.

So, okay. If you just type "netstat" now and hit Enter, you'll get sort of a – begin to get comfortable with what's going on. And I will encourage you not, you know, encourage everyone not to freak out. I mean, it looks complicated, and it's got all kinds of stuff going on, but we're going to sort of tackle this step by step and simplify this so that it's pretty clear what's happening.

Leo: Look, I actually – I can see that I'm connected to Irvine, which I presume is you.

Steve: Oh, yeah, I'm sure it is. And, see, that's what's so cool is that, say for example that you were going over to a friend's house because something was wrong with their computer, their modem light was flashing all the time, you know, their cable modem or DSL, or had gotten really slow, I mean, and the first thing you want to know is, okay, what's happening here with this computer?

Leo: Should I be concerned that I'm connected to France? Maybe we'll get to that a little later on.

Steve: Well, I mean, and this is the beauty, is remember that we're not here to, like, scare people. We're here to give people tools that they can use to answer these questions themselves. I would say, Leo, that if you didn't expect to be connected to France, then you will want to find out why you are.

Leo: Why I am.

Steve: So, for example, right now you could type "netstat □b. " B stands for binary. That will add to the display the names of the programs that are responsible for every line in that Netstat display.

Leo: Ah, okay.

Steve: And what that'll allow you to do is to find out which executable program in your system...

Leo: Skype.

Steve: Oh. Interesting.

Leo: Am I a supernode? Is that what that means?

Steve: Well, let's hope not. No, I would think you're behind a router, so...

Leo: I am.

Steve: Or you've opened a hole.

Leo: I've opened up a port in order to make this usable. And I see that somebody in Grenoble, France, is using me, as well as LAX, San Francisco – I think probably these are you, they're Comcast.net. I don't – all of this is on Skype. This is interesting.

Steve: Well, aren't you glad about Netstat. I couldn't ask for a better example, Leo.

Leo: I will take a screenshot and show people because that's...

Steve: People are going to think we're making this up, or we set this up.

Leo: I'm not.

Steve: No, I know. And in fact I once went to a home of some people who were having some

serious problems with their machine. I think I referred to them before. There was a machine that was sending traffic to us, located in Irvine. I went through the FBI to get their name and address, and the FBI contacted them and said, would you mind if one of our friends came over and took a look at your computer?

First thing I did was open a DOS box, type "netstat," and it was like, oh, my God. I mean, they had so much crud in their machine, and a whole bunch of connections to 6667, which is the default IRC port. So, for example, if you say "netstat," and you see 6667s, there's a very good chance that – and you're not knowingly using IRC – there's a chance that you've got an IRC trojan that has connected to a remote IRC server and is connected right now and waiting to receive commands, following, you know, exactly what we were talking about before about the whole bot armies and bot fleets and how all that works.

So the beauty of this is it's built into the system, it's always there, and you don't have to load or install or bring any software with you if you want to find out what some computer is doing.

So in general the Netstat display has four columns. The leftmost column says Proto, and that's short for protocol. We've talked about TCP and UDP. Netstat always sorts the protocols so that all the TCP connections and activities are shown first, followed by UDP. The second column is the Local Address column. Now, we've talked about how a socket is an IP address and a port. So what you'll see there is either an IP address, you know, the standard something.something.something.something. For example, if we're looking at the Local column, you might see your machine's own IP address, 192.168.something, you know, .0.1 or whatever, then a colon and the port number. So the way the so-called "socket" is displayed, the socket endpoint, to use the full terminology, is an IP address and colon and then the port number that is involved in that. You may see things that say 127.0.0.1. We talked about that with regard to the hosts file recently. That's called the Localhost IP. That's sort of an abbreviation or just another IP that represents your own machine.

Leo: I see that a lot on the Mac. I don't see it on my Windows machine particularly.

Steve: Yeah. Also over on the Local side you might see 0.0.0.0. That's actually a wildcard IP. That means, you know, any IP. So, for example, if you have some lines that show LISTENING when it displays – actually, if you just type "netstat," like even "–b," you won't see any lines that show LISTENING because the normal Netstat command just all by itself only shows you either existing or recently closed connections. You need to say "–a." "A" stands for all. Then you'll see – so if you say "netstat -a," or over on the Mac you'd say "netstat -finet" and then " -a," now you will also see any listening sockets. These are...

Leo: That's a lot longer list, too.

Steve: Yeah, it is a lot longer list. And these are so-called "open ports." These are ports on your machine due to processes running in your machine which have opened ports and are looking for incoming traffic. Now, people should not freak out because this, remember, is the machine itself, that's inside the firewall that might be running on your machine, and hopefully is if you don't have any other protection, and it's inside your NAT router. So the fact that these are open listening ports on your computer does not mean that they are exposed to the public Internet.

Leo: Let's mention a couple that you might see a lot of For instance, svchost.exe. I see that all the time when I run software firewalls. They say svchost is trying to connect. What is that?

Steve: That's a general sort of a generic hosting process that contains a whole collection of Windows services.

Leo: Ah.

Steve: So it's an executable that is sort of like a potpourri. The way Windows works, you're able to have multiple services in a single executable. So it might be DNS. It might be your NetBIOS technology. It could be any of the services that you see when you enumerate all of the services your system is running. Many of them are sort of collected inside a single svchost.exe file.

Leo: Right. And there's also LSASS. You see a lot of that.

Steve: Yes. That's the licensing security service service.

Leo: And of course Sasser took advantage of that and named itself LSSASS.

Steve: Right, right.

Leo: And that was a sign you had Sasser. So let's hope you don't see that.

Steve: In Windows you'll often see port 135, so you'll see something that is :135. I ought to also mention, I mean, I intended to sort of get to the...

Leo: Oh, I'm sorry, I interrupted you, yeah. We're going to do the columns. We were doing the columns across.

Steve: Well, yeah, because then we'll talk about command line options.

Leo: Okay.

Steve: Because you're probably seeing things like DNS and NETBIOS dot, you know, various English versions. If you do –n, "n" stands for "numeric." Then you'll see these things in numeric form rather than having them sort of trans- Windows translating them into something easier. And I don't know, I'm just comfortable with port numbers because I know 53 is DNS, and 135 is RPC and so forth.

Leo: Right, right.

Steve: Okay. So we have the first column is protocols, second column is the local endpoint, and the third column is the remote or the foreign address. Well, that's the one that's really interesting because this – and I'm sure this is where you've been seeing France and Irvine and San Francisco and so forth. These are the IP and port to which your computer is connected at

the moment. You'll see that if you do a netstat –a for all, which will show you listening, then you'll see 0.0.0.0: and a port, meaning that it will accept any – it will accept a connection incoming from any IP, 0.0.0.0 being sort of a wildcard, sort of like *.* is in our file system.

And then the final column is called State, which is the state that this connection or potential connection is in. Most common states are LISTENING, meaning that you have an, I mean, a classic open port listening for any incoming traffic. If you actually have connections established, that is, you know, I mean, that's what was – we've talked about the TCP three-way handshake that establishes a connection. And so now you have an agreement between your local machine and some remote machine. Then the word ESTABLISHED will appear in that column, meaning that that is an actual connection right now that exists between your machine and that remote IP and port that is able to exchange traffic. And sometimes people will see TIME_WAIT. TIME_WAIT is a state that TCP goes into at the end of an established connection, as it's being torn down, that prevents packets coming in late from confusing the system. So it's sort of like a delay before those endpoints can be used again. It sort of holds that connection out of use to allow the packets that might be still floating around the Internet to die or no longer arrive before it will sort of release that for re-use so that a new connection isn't confused by an old connection's, you know, similar endpoint packets coming along.

So generally you'll see LISTENING, meaning you've got open ports and something is listening for incoming packets to accept a connection; ESTABLISHED, for an existing connection; or TIME_WAIT for one that was just connected but is no longer connected. Then less common are sort of more of the TCP plumbing. Sometimes you might see SYN_RECEIVED or SYN_SENT that literally refers to the SYN packets we've talked about often that are involved in establishing a connection. So that means that a connection is in the process of being set up. And normally that happens so quickly that you won't see it in a Netstat command. But I've seen them, and in fact on a busy server you typically will see them. You may also...

Leo: Now, Netstat isn't always updating itself, though, right?

Steve: Actually Netstat doesn't. It takes a snapshot right then. There is a command line option that – I think it's "i" for interval – that allows you to say, you know, do this...

Leo: Keeping doing it.

Steve: Yeah, exactly, do it repetitively. But that's one of the cool things about TCPView. Basically everything I've talked about here applies to the GUI version of this that Mark wrote at Sysinternals, TCPView. And it has a very nice feature where it does automatically update itself, I think it's about every five seconds. And you can control that interval. And even cooler is it will highlight with a green and a red highlight on the line as new things are added and as old things go away, to sort of draw your eye to the changes that are occurring in this list.

So one thing that people could do if they wanted to experiment with this would be to open their web browser and do a little bit of web surfing, maybe jump to a few different sites, and then do a Netstat command over in their DOS box. And you'll suddenly see a bunch of stuff that wasn't there before. You'll see established connections and time_wait, that is previously established connections, right there in the display. And you'll see the IP address and port, or maybe even the host name, that is the domain name and port, if the system is looking that up for you.

So the final thing you may see, there's one fifth column called PID, which is the Process ID. People who have used Task Manager before may have turned on the column that shows you the process ID of the various programs. This is a sort of a universal token which the system uses to identify and essentially to number all the processes that are running in it at any given time. There are some command line options to Netstat which produce additional information

we'll talk about next. And that also causes this PID, the Process ID column, to display, although it's not particularly useful information unless you have some use for, like, associating that with the Task Manager display.

Leo: Yeah, it's more useful to UNIX folks who can then list processes and kill processes and that kind of stuff.

Steve: Right. So in terms of command line options, so now we've got a DOS box, we've got the window open, we've got our scroll so we can scroll back if this thing is long. You can always, over on the Windows side, you can always say "netstat /?," sort of the standard tell me, you know, what commands to use, so the way of asking for, like, online help for the Netstat command. This is important because, for example, Windows 2000 has a different set of commands than Windows XP does. XP has added some really nice new features. And since most people are over on XP, that's where I'm focusing. And so if this doesn't work, if some of the things I'm talking about, for example, Windows 2000 does not show you the processes associated with the line items that Netstat has. There is no –b for binaries, so you're not able to do that. So you might want, over on Windows 2000, do "netstat /?," and that will show you which command line options are available in your version of Netstat. And this even works on Windows 98. I mean, Netstat has always been there since the TCP/IP stack arrived over on Windows. So...

Leo: It's interesting because Windows has a number of command line utilities, and always has, like ipconfig and Netstat, that are very useful; but I think people don't really know they exist unless they have to troubleshoot a network connection or something like that.

Steve: Right. Well, it's funny, too, because, I mean, I had never given the "man netstat" command to a Mac.

Leo: Isn't that great.

Steve: And I was thinking, gee, I wonder, you know, does the Mac have the full set of manuals? And...

Leo: Well, it doesn't have the full set, but it has a lot of manuals for a lot of...

Steve: Yeah.

Leo: Yeah, it's very handy because you can always find out more about a program.

Steve: Right. So over on Netstat we've talked about the –a command, "a" stands for "all," whereas where Netstat normally shows you only established connections, in order to find out what ports are listening and what services are associated with those listening ports, you need to add an "a" to the command line options, "a" for "all," and then you'll see a lot more information. The –b command for over on Windows XP also says show me which binaries, that is, the executables, are responsible on a line-by-line basis for being involved with this particular element of the stack, either something listening or something that has a connection in your machine. And that's very valuable because it'll give you the application name. It's good if you at least know what it is. For example, Leo, I'm sure you saw Skype.exe.

Leo: Yeah, I mean, that's pretty obvious.

Steve: Yeah, exactly, you know what Skype is. Now, on the other hand, you're not sure why it seems to be connecting all over the planet.

Leo: But that's a start. I mean, at least I know who's connecting.

Steve: Exactly.

Leo: Can you spoof that information? I mean, I guess you could if you named yourself Skype.exe.

Steve: Exactly. In fact, that was what my original LeakTest program, you know, I wrote the first firewall leak tester that anyone ever created, just called it LeakTest. And what I realized was the firewalls were – the early firewalls were saying, hey, we're going to make sure that only applications you permit are able to use your Internet connection. It's like, well, that's good. But at the time there was only one firewall, that was also at the time my favorite firewall, ZoneAlarm. Of course that's no longer true. Now I'm a Kerio fan. But only ZoneAlarm was actually checking basically a cryptographic fingerprint of the application. They were doing a hash to make sure that it really was the same application you had given permission to. So all malware had to do was call itself Explorer.exe or, you know, or IExplorer.exe, to masquerade as Internet Explorer. Everyone would have given Internet Explorer through their firewall, or they wouldn't be able to web surf.

And so anyway, my little LeakTest became very popular. And within a very short period of time every firewall manufacturer was virtually forced by their users to add this feature. And now no firewall doesn't check to make sure it's really the application that you gave permission to.

Leo: So presumably, because of fingerprinting, when Netstat says it's Skype, it is Skype.

Steve: Actually, no. Fingerprinting wouldn't prevent that forgery at this level. It would prevent it from getting out of your firewall if you were running a personal firewall on your machine.

Leo: So there is no protection that this is actually Skype when I'm looking at it in Netstat.

Steve: That is true.

Leo: Okay.

Steve: That is true. For example, what you could do is, well, for one thing, if you weren't running Skype and it said Skype is doing this, it's like, uh, I don't think so.

Leo: Yeah, I don't have it.

Steve: And what you could do is – but don't do it now, Leo, because we are using Skype...

Leo: Like before, you mean.

Steve: You could close Skype and then run Netstat again...

Leo: And see what happened, right.

Steve: Exactly, see if all the Skype entries went away, as you would expect them to. So, I mean, this is an incredibly powerful tool that I'm really glad we're talking about because, for people who want to know what their computer is doing, this does it.

So just to finish with these couple last command line options, "a" for all; "b" for showing binaries; "n," instead of the normal display, it tries to do DNS lookups for the IPs, which is useful by default unless you want to see what the actual IP and port number is. You can get that by saying "n," which is short for numeric. So that says give me this display in just numeric form, numeric IPs and ports, instead of, you know, friendly human domain names and English versions of the port, like DNS instead of 53, for example.

Leo: Is there any reason, any time you'd prefer that over the English language?

Steve: I actually do. I always...

Leo: You do because you know the numbers.

Steve: Exactly. But so anyway, it's there as an option.

Leo: Even if you know the numbers, though, you don't know some of the Internet addresses. So the reverse lookup that it does on that is very useful.

Steve: Very good point, yes.

Leo: Yeah, yeah.

Steve: And the last one is a "v" option. Now, I couldn't think of what "v" could possibly stand for, except perhaps very much more than you ever wanted to know.

Leo: Verbose is what it stands for.

Steve: There you go, that's exactly what it's for, yes.

Leo: Yeah. That's a lot of UNIX commands. It's noisy. The noisy version.

Steve: Oh. Well, in fact, oh, in Windows XP it is that to an extreme. What it does is it shows you, not only which executable is behind what's going on, but then in reverse order it shows you the hierarchy of internal Windows modules which have been invoked in a stack, in a chain essentially, all the way back down to the lowest level it can get. So, for example, Skype is probably invoking something else, which is invoking something else, which is invoking something else. So I would imagine – I'm not doing it. I'm sure you can, Leo, if you were to do...

Leo: I'm doing it right now, and it's gone on for quite a while.

Steve: Yeah. It just – it's, like I said, very much more than you ever wanted to know. And I don't really think that's very useful, except for real serious computer guys. If you didn't recognize what your application was by name, it might be that something it was calling would be more familiar, although you'd still need to know what that main binary was that was, you know, starting up all of this traffic.

Leo: Right.

Steve: So that would be very useful. So you can also concatenate these. For example, you could say "netstat □abn, " or "abnv" just all running together, in order to put those together. Or probably just "ab." I would think that's probably going to be the most popular collection because that's going to give you all of what's happening and tell you what the binaries are. So you'll be able to see who is doing connections, who is listening to ports, and what's going on.

Leo: Yeah, that's the one I use pretty much exclusively.

Steve: Yep, "netstat ab."

Leo: Space dash ab.

Steve: Yes, exactly. I think slash or dash, both work.

Leo: Oh, okay.

Steve: So either way. Anyway, there is a short course on Netstat command, a very useful command which can be used – you know, again, no software needs to be installed. It's available in any machine you approach. You want to know what's going on, this thing will tell you. And again, remember that listening ports are ports that are open on your machine internally, but not any which are exposed externally. If you wanted to find out for sure, you could use ShieldsUP!, you know, at my GRC.com. You're able to use the custom port probe feature that GRC has. You can put in any ports that you want specifically checked, and I will send from GRC servers probes back to your IP at those ports and tell you whether they're open or closed. So you're able to do a custom port probe that way. Or just do the normal full service port scan, which doesn't take very long, that tests ports 1 through 1056, I think it is, that I'm

testing.

So again, ports that are shown internally are not necessarily exposed, but they do represent something in your machine that would like to have the opportunity to talk on the Internet. So, for example, you could have a trojan in your machine which is not detected by any external software, like that ShieldsUP! won't see because you're being protected by a router or by your software firewall. Nonetheless, you've got a trojan, you might have a trojan which has opened a port, a back door, that is wanting and hoping for someone to connect to it.

Leo: So it would be listening, then.

Steve: So it would be listening. And so this is still very useful information because it shows you what's going on that would like to be having a conversation. Even though it can't, you may want to get rid of it. It may be something you don't want in your computer. So again, this Netstat command is, like, the way to do that.

I also fired up Kerio, the Kerio firewall, briefly because I was sure that I remembered that it had built in its own very nice connection monitor. And I wanted just to verify that it did, and indeed it does. In the Overview there is a Connections tab. And Kerio itself will show you all of the current connections that it has through itself. So there's another way, if you happen to be using Kerio and it's installed, to see what's going on.

Leo: That's free as well, from Sunbelt-software.com.

Steve: Exactly. But again, it's something that you have to install, and the Netstat command is sort of a superset of that because it'll show even things that are listening and haven't yet been able to establish a connection.

Leo: Now, here's a question for you. If I have a rootkit, like the Sony rootkit, and it's listening, is it visible in Netstat?

Steve: Well, I don't think the Sony rootkit was opening a port and listening. So I wouldn't say that you could count on Netstat, for example, like to be a comprehensive process list that would show you all the processes running.

Leo: Well, I know in fact a rootkit would not show up in the process list. I wonder if it would show up, though, in the Netstat list as making a connection.

Steve: Well...

Leo: I guess it must have had its own stack. If it had its own stack you wouldn't see it.

Steve: It would be a huge lot of work to circumvent the stack and get down to the adapter, but you certainly could. For example, there are network monitoring tools which install a low-level driver that allows them – that allow them to sniff the network traffic. And they don't show in Netstat.

Leo: Right.

Steve: So it is really for things that are playing by the rules and behaving themselves. And I think I see why you've raised the point, Leo, and it's a very good one. This is not a guaranteed display of absolutely everything going on. Because it's running in – and this is, you know, one of our standard laws of security – because it's running in the same computer that you're questioning whether something malicious might also be sharing. There's just – there's no way you can ever trust anything in the same machine as the one that might be hosting something malicious. There just isn't a way.

Leo: And that's why people will use programs like Nmap from outside the machine to check those kinds of connections.

Steve: Well, yes. And in fact we talked last week about the idea of – and this was one of the questions raised in last week's Q&A. Someone was asking, you know, how can I be really sure about what's going on? And the answer was, well, you can use a program like Netstat, a command like Netstat, to probably see what's going on. And it's certainly super useful in 99.999 percent of the cases. But to really know, you would have to be running your machine's traffic through another machine and be watching the traffic there. Or perhaps have a an external firewall or router which is showing you what connections and traffic it has alive and open at any given time. But you lose then, as soon as you step outside the machine, you lose the ability to know which programs are running inside your machine.

Leo: Right.

Steve: And so I'll say lastly that Sysinternals has this program, TCPView, which is freeware. There's a Pro version which is not free but not very expensive. If you love TCPView you can look and see what the additional features of TCPView Pro are. One of them, for example, is that in earlier versions of the OSes – 95, 98, I think in 2000 – there is – the TCPView won't show you the processes running. TCPView Pro does. Which is, you know, as we've said, is very useful to see who is listening, who is opening ports and established connections. TCPView Pro will do that for all versions of Windows operating systems. And again, it's, you know, if you get comfortable with Netstat, the actual command line that we've been talking about, and then run TCPView, even the freeware version, you'll see it's exactly the same sort of display. It's very comfortable. And it allows you just to kind of keep an eye on what's going on in your computer from moment to moment. And very handy.

Leo: If you want to keep an eye on what's going on in your computer all the time, may I recommend our lovely sponsor, the Astaro Corporation, makers of the Astaro Security Gateway. If your small or medium business network needs superior protection from spam, viruses, hackers, as well as complete VPN capabilities, intrusion protection, content filtering, and an industrial-strength firewall, all in a very easy-to-use, high-performance appliance, I want you to contact Astaro, Astaro.com, or call 877-4AS-TARO. You can schedule a free trial of the Astaro Security Gateway appliance in your business. And of course if you're a noncommercial user you can download the software, ASG for home use, at the same site, Astaro.com. We thank them for their support.

And as long as we're giving plugs out, we can't forget to plug our good friends at GRC.com. That's Steve's site. You know, you were talking about how Mark and Sysinternals have been giving away all this great software, and everybody loves it. I was just thinking you've

done much the same thing. You have a lot of very useful free utilities that you've put out there.

Steve: Yeah, well, you know, I've written things that there's been a need for. There was, you know, when firewalls weren't checking, as we were talking before, that the real program was what was happening, the program might be masquerading as a different filename, I wrote LeakTest.

Leo: Right.

Steve: When I discovered that Aureate spyware, I wrote OptOut to be, you know, the very first spyware eliminator, detector and eliminator. And then of course through the years I've continued to write freeware...

Leo: Just more and more, yeah.

Steve: Exactly.

Leo: DCOMbobulator, Shoot The Messenger, UnPlug n' Pray...

Steve: Well, in fact, you and I first met at TechTV when I had TIP, Trouble In Paradise.

Leo: Yeah, the Click of Death.

Steve: The Click of Death for the Iomega cartridges.

Leo: You've always been a boon. Anybody who wants to know more and should – everybody who's testing their security should be trying it through ShieldsUP!. It's GRC.com, you'll see a link there for Shields UP!. And of course Steve's bread and butter, the fabulous SpinRite, which is everybody, including me personally, my favorite disk recovery and maintenance utility. You know, if you're interested in information, you know, it's fun to look at Netstat; but you want to find out more about what your hard drive's doing, just run SpinRite. Unbelievable. You...

Steve: There's a lot of information there.

Leo: You showed me, and this is something everybody should try out, just watch how many error corrections a second your hard drive is doing.

Steve: Yes.

Leo: It's a lot.

Steve: Well, and actually it's fun because the ECC used to be something that was only being done in the event of, like, a problem with a sector that needed to be relocated. Now drives' density has gotten so high that ECC is happening on the fly all the time.

Leo: All the time.

Steve: But what's neat is that it creates a very useful early warning system. If the rate, that is, the level of ECC started to increase over what it was when the drive was new, that would be an early red flag that the drive was having more trouble.

Leo: Certainly something, yeah...

Steve: And SpinRite will show that to you.

Leo: It's interesting, but it's a great diagnostic. SpinRite is really, I mean, anybody who works with hard drives knows, I don't have to tell them. But for those of you who are new to this or have a problem hard drive that you want to recover or just want to know more, SpinRite.info. That's all the testimonials and a link to where you can get a copy of SpinRite for yourself from GRC.com.

We have come to the end of, I think, one of the most interesting shows. I think Netstat is such a useful tool. And I love tools where you can investigate your system. I know users do, too.

Steve: Well, it's a little daunting when you first give the command. But if people will not run away from the screen, just sort of sit there and go, okay, now, wait – well, and in fact, I think if people do "netstat –ab," they're going to see a bunch of stuff. And just like you did, Leo, it's like, okay...

Leo: Whoa, what's France?

Steve: ...what's going on?

Leo: Why is France connecting with me? No, but exactly. And you know, that's what we're all about. This show and, in fact, all of the shows on TWiT.tv are not aimed at people who just want to use their computer and not curious about it, not interested in how it's working or what it's doing. But we're aimed at people who are curious. And if you're interested in your machine, this is just a great little tool. I think everybody who listens will want to know more.

Thank you, Steve. Reminder, we've got a brand new site, TWiT.tv, all new, fresh, and shiny, just for you. The paint is dry.

Steve: It looks really nice. Really nice, Leo.

Leo: Yeah, and it's much easier, I think, now to find the podcasts. And listen to them right on the site with a great Flash player that was designed by Mike Hogue. So thank you, Mike, for that. And there's also the donation buttons, and we certainly do appreciate your donations. They are what keeps this podcast afloat. Just to make it clear, you know, we do have advertising. That money goes to the podcasters, the contributors, as salaries. The money that you donate goes to infrastructure, things like the web design, the bandwidth, the web hosting, the rental for the offices, the equipment, all of that stuff. And those expenses are not minuscule, trust me. We really – your contribution has made this network possible, and we really do thank you for that. TWiT.tv.

And now, my friends, the time has come to say goodnight to l little Stevie Gibson.

Steve: For one week.

Leo: For one week. Next week?

Steve: Next week is we're going to plow into a really interesting topic, which is virtual machine technology.

Leo: Oh, I'm excited, we're going to begin that. That's going to be a two-parter, isn't it.

Steve: It's going to be a multi-parter because it's extremely useful, and I want to lay down some foundation. Again, I want to approach this and really fully cover it because, for the growing concern of security, virtual machine technology allows true sandboxing and encapsulation of potentially dangerous Internet experiences in a way that won't allow anything that happens to affect anything outside the sandbox. Nothing can get to your machine. So some really cool stuff there. And we'll start talking about it next week.