# SECURITY NOW!

Transcript of Episode #147

## Microsoft Baseline Security Analyzer

**Description:** Steve and Leo discuss the recent hacker takeover of the Comcast domain, then examine two very useful free security tools offered by Microsoft: the Baseline Security Analyzer (MBSA) and the Microsoft Security Assessment Tool (MSAT).

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-147.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-147-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

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

This is Security Now! with Steve Gibson, Episode 147 for June 5, 2008: Microsoft's Baseline Security Analyzer. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

It's time for Security Now!, time to talk about keeping yourself safe and sound in this modern time. And what better person to do that than Mr. Steve Gibson of GRC.com? Good morning, Steve.

**Steve Gibson:** Hello, Leo. Great to be back with you again.

**Leo:** To talk about saving your butts. Security.

**Steve:** Yeah.

**Leo:** Yeah. I was having a long conversation on the radio show - this comes up a lot on the radio show, security, how to protect yourself. Fellow asked, and I think it was a reasonable thing, he'd run a security scan and came up with four different kinds of critters: adware, spyware, rogue software I think they called it, and trojan horses.

**Steve:** Rogue, I like that, it's roguish.

**Leo:** Well, I told him, what I said is nowadays I think it's all malware. I mean, I don't think that there's much distinction between adware, spyware, and viruses. They all act the same.

**Steve:** Well, "mal" as in something that you really don't want on your machine. You just don't want it around.

**Leo:** Well, anyway, he was panicked, as all people are. And, you know, sometimes I get in this battle about whether you should format the drive or if there's some way to do it without formatting the drive. But every time I talk to somebody, you know, in fact there's a guy on Twitter said, oh, you always say format the drive. You don't have to format the drive. I asked him, I said, well, what percentage of malware infections are you able to get rid of without formatting, and how many of them come back? And he said, well, you know, 99 percent of them come back. And it seems to me that you have to format the drive.

**Steve:** Yeah. In fact, there has been some evolution there. Remember that - I remember clearly when we were talking about this at one point, you know, in the last three years, the formal rule is, if your machine has been compromised, you can never trust it again. There isn't any way to know what it is that was changed. And in fact when, you know, I've talked to some people who are sort of old-school sticklers for, oh, I know what every single file on my machine is, you know, back from the DOS days. And there have been some friends who have spent weeks trying to get stuff removed after an infection. And you really cannot do it.

It turns out that, I mean, the way this malware has evolved now, it's so insidious and sinks itself so deep into the system and, you know, renames files and sticks itself in places you don't know to look and is able to hook itself in so that it gets started up in many different scenarios, I mean, if you get a serious infection, really, I mean, for two reasons. First of all, you don't ever - you will never again, by definition, be able to trust the system. And secondly, you just can't get rid of it. It won't go away. And when people say, well, it comes back, what it means is they didn't get rid of it the first time. There was some little hook left somewhere, some little piece of evilness that is monitoring, and it reinfects the system. So it's just - I think your advice is right, Leo. You just - mostly, how could you ever do ebanking on a machine that once had this on there? I mean, there just isn't a way you can trust a machine that was taken over.

**Leo:** Karoli asks in our chatroom, well, what about System Restore, is that enough?

**Steve:** Well, there are now System Restore-aware malware. Which, I mean, that is a great example of the adaptation that we're seeing in this kind of malicious software is that it's evolving step by step. Once upon a time, remember, the spyware scanners could remove spyware. They'd say, okay, we got rid of it, and it would be gone. Now all kinds of things break because the software is really insinuating itself into the system because it doesn't want to be removed. And it's successful in not wanting to be removed. So even System Restore - and the problem is System Restore is sitting on the same system. If it's in the same system, you can't trust it.

**Leo:** Frequently, in fact, people will restore viruses that they got rid of.

**Steve:** Right.

**Leo:** Isn't that nice.

**Steve:** Right, yeah. So, I mean, the only thing that would make sense that you could trust would be if you had offline images, and you reimaged your system from an offline image that occurred before the problem. As we know, the best solution is not to have the problem in the first place.

**Leo:** Well, let's talk about security news, as we always do. And then we're going to get into our topic of the day. What do you want to talk about today?

**Steve:** I want to talk about two utilities that Microsoft offers. We had a great response to talking about Secunia's Personal Software Inspector, which talks about third-party software. Back when Microsoft got all into security, they produced a couple of tools, one called the Baseline Security Analyzer, which is an interesting, sort of Secunia-like tool. And the second is called the Microsoft Security Assessment tool. So I want to introduce our listeners to that. You'll have links to them. I've got links to them on our show notes. So people can experiment with them. They are, again, they're not something you would get with Windows Update or automatically. You've got to go to Microsoft and get this. But they're both interestingly useful, I think. And I think our users, our listeners of Security Now! would find them useful, as well.

**Leo:** Cool. So we'll talk about that in just a bit. Any big security news?

**Steve:** The big news, I mean, the really big news actually occurred after we recorded last week's...

**Leo:** Of course. Probably seconds afterwards, yes, of course.

**Steve:** We record on Tuesday, of course, and then air the show on Thursday. In that intervening period, Comcast got their DNS record, essentially, hacked. What happened was that somehow, from looking at all the evidence, it looks to me as though that someone malicious inside of Comcast is my best guess, maybe it's an ex-employee, someone disgruntled, it's impossible to know exactly what happened. But on Comcast's domain, Comcast.net, is hosted by, well, their registrar is Network Solutions. There's no indication that Network Solutions themselves were hacked. But the registrar record for Comcast.net was definitely hacked. There's a bunch of, you know, script kiddoe-ish lingo in the administration contact. They repointed the primary and secondary Comcast name servers, which are normally Comcast-provided servers. They redirected them to ns21.worldnic.com and ns22.worldnic.com, which are the name servers that Network Solutions supplies. And those pointed to a bogus server, I believe it was in Germany.

Now, this basically, I mean, this took Comcast.net off the 'Net for the period of time that it took them to find the problem, change the record, and then for DNS changes to propagate. So, and it's interesting, too, because I got email from my office manager, Sue, on I think it was Thursday evening or maybe Friday morning saying that a bunch of our eCommerce receipts sent by our eCommerce system had bounced. And she had noted they were all Comcast.net. So there was some mistaken reporting, unfortunately, by the nontechnical press, saying that it was only Comcast's portal, that like people who were...

**Leo:** That did get hacked, though, I mean, there was some text on there, hacker text and so forth.

**Steve:** Well, this is all part of the same thing, well, unless it was related and different. It may have been, for example, that some password file that Comcast maintains got out and so someone was able to hack the portal. But what did happen was Comcast.net got redirected to a different server that was putting up a hacker-esque message. But this was...

**Leo:** Now, they're saying they think they know who it was, and it's these, you know, Kevin Poulsen interviewed these two high school dropouts who say, yeah, we found a security flaw in Comcast, and we probably should have told them, but we just thought, well, what the heck, we'll take advantage of it.

**Steve:** Okay. Well, again, they may have gotten into Comcast's network, found the information, and then been able to log into it. It looks to me as though someone got the logon credentials for Comcast's Network Solutions account and then went there and changed that information at Network Solutions, which then redirected Comcast.net to a different pair of name servers from Comcast's, and from there they were able to do, you know, play any games they wanted to. Anyway, if it happened to TonyNoodles.com, no one would have cared.

**Leo:** It happens all the time to TonyNoodles.com.

**Steve:** Exactly.

**Leo:** It happened to me. I mean, you know. So this is according to Kevin Poulsen's article. You know, Kevin was a hacker himself but did some jail time. We've interviewed him many times before. And now is actually a very credible, really good reporter. He's an excellent reporter. And by I think because of his connections with the hacking community he was able to talk to these guys. They respected him. He said he had an hour-long conference call with this hacker group called Threat Level. And the hackers - oh, no, I'm sorry, they talked to Threat Level. The hackers' names were Defiant and EBK. And it was a DNS hijack, as you say.

**Steve:** Yup. And in fact Defiant and EBK name is in the edited administrative contact in Network Solutions.

**Leo:** Yeah. And Threat Level, which is the blog that Kevin writes, says he did verify their identities. They wouldn't say where they were. His MySpace profile, Defiant's MySpace profile says he lives in Cashville, Tennessee. I don't think that's accurate. Network Solutions said it had nothing to do with us, there was no breach in our system, no social engineering. Of course they're going to say that. Who knows what really happened. But as you said, it was a transfer of the account to them. I always worry about that. You know, I mean, we have - when you register a domain, most domain registrars will allow you to lock it down so that these can't - there can't be administrative transfers. They make it very difficult. But still, you know, ultimately with a fax and maybe some phone calls you can get that stuff transferred over; right?

**Steve:** Well, and look at what's happened. Once upon a time, like in the beginning of all this, 15 years ago, it would have been uncomfortable if you couldn't get email for a day or something. But what's happened is...

**Leo:** This is serious, yeah.

**Steve:** Exactly. In the intervening time we've built, you know, a mission-critical economy on top of all this. And the underlying structure, while it's been strengthened a little bit, it's still prone to, as you said, social engineering hacks and various types of malicious conduct. And it's now not a small thing if this happens. It's a big deal. You can imagine how Comcast feels. I mean, their whole network would have been messed up for many hours because any DNS servers whose cached Comcast.net records timed out, they would have gone back to the root server to update, to refresh their DNS. If they did that during this window where the record was changed, they would have picked up the malicious record. And even after Comcast fixed it, those servers would still have the wrong information and would have no reason to go back and reverify it.

**Leo:** How often do they do that? They do - it does expire after a while; right?

**Steve:** Yeah, typically it's a day, though, because you don't want to load down your DNS server too much. So oftentimes it's - especially in a situation like with Comcast, where they have no expectation or intention of needing to change that information. So, for example, one of the things that is often done for a site that they're under a heavy DoS attack is they'll deliberately bring their record expiration down maybe to an hour, maybe even to, like, ten minutes because that gives them the flexibility of changing their DNS in a much shorter period of time. But typically it's about a day. So anything that had happened to expire during that window where the records were wrong, the authoritative DNS records were wrong, servers would have gone back and picked up the new information and kept it probably for a day. So it was about a day-long problem before this thing got itself cleared out.

**Leo:** They said that they tried to tell Comcast, but they wouldn't listen. Yeah, I bet. I don't know why I don't believe that. What else is in the security news?

**Steve:** Well, two things. I did want to mention to all of our Mac listeners about the major

OS X update, 10.5.3, because although it didn't get a lot of press attention, there were a number of remote code execution vulnerabilities which...

**Leo:** Well, we talked about them last week, I think the Macintosh vulnerabilities; right? And we [indiscernible] fixed it.

**Steve:** We talked about the iCal vulnerability.

**Leo:** Right. And I think they - we don't know. You know, I looked at the update immediately when it - because the update came out Tuesday.

**Steve:** Right.

**Leo:** And I immediately looked at it, said has this been fixed? And it doesn't say.

**Steve:** Yeah. What I have seen is that there are still some iCal issues that have not been fixed. Specifically two known problems that Apple has not yet addressed. And then the last thing I wanted to mention was there is an exploit in the wild for a known vulnerable version of the Adobe Flash Player. Version 9.0.124.0 is the latest and the current one. Secunia knows about it. So if you downloaded Secunia two weeks ago, you can just check, during our episode about that, you can check in with it. I've just checked my systems, and I did have 9.0.124. But I remember that it was Secunia that had alerted me to the fact that I was behind and that there was a problem. I mention this again because there are now Windows-based exploits in the wild.

**Leo:** Oh, boy.

**Steve:** Apple's fix from last week does address this. So there were problems with Apple's version of the Flash Player, as well, but they fixed that in their mega, you know, 200MB OS X update.

**Leo:** Now, you didn't mention, I'm kind of surprised at you for not mentioning it, that there was a little bit of a DoS attack against our friends at Revision3.

**Steve:** Oh, that's very true. I didn't really follow up or know any details. But I was talking to Mark Thompson, and he said that they were seriously under the weather.

**Leo:** Yeah. Jim Louderback did, I thought, a very good job. We have Jim and Patrick and Martin Sargent on TWiT, and so we talked quite a bit about it. Jim did a very good job on his blog talking about it. But let me tell you what happened. It's kind of interesting. It was a SYN flood. Jim does a great job explaining SYN floods. We've talked about it before on this show. I think anybody who listens to this show probably knows what a SYN flood is. But it was kind of unusual in the sense that they didn't hide the source of the SYN packets. They were getting 8,000 SYNs a second, which took Revision3 down for the entire Memorial Day weekend. But it was apparent where it was coming from. It was coming from MediaDefender, which is a company run by or funded by the recording industry in order to bring down torrent sites.

What MediaDefender does is they create fake bit torrents of illegal content, movies and music, and then seed the torrent trackers with that so that people can't find the legitimate, or illegitimate legitimate stuff and end up, you know, getting non-downloads. They also apparently, as part of their portfolio, do DoS attacks against BitTorrent trackers. Revision3 was running without - kind of they really had forgotten about it. In the early days of Revision3, I mean, really early days, three years ago, they used BitTorrent to distribute Systm and some of their other programs. So they were running a BitTorrent tracker. It had - Jim explained this. But apparently it had become open over the last couple of weeks, which means that other people could put other torrents on there instead of just the Revision3 shows. And MediaDefender says there were 296,000 other torrents on there.

But here's the funny thing. It was open. It was out there. MediaDefender was using it as one of their trackers that they seed with the phony torrents. Then Revision3 found out it was an open tracker and closed it, and that triggered the attack. MediaDefender started SYN flooding it after they closed their open torrent tracker. It was almost a retaliation for closing the tracker.

**Steve:** Okay. I'm curious, then. Because doing what they did, for MediaDefender to do what it apparently deliberately and intentionally did to Revision3 is against all kinds of laws.

**Leo:** It's illegal.

**Steve:** I mean...

**Leo:** [Indiscernible].

**Steve:** Absolutely illegal.

**Leo:** Yeah. So it's a little puzzling. I asked Jim, are you going to sue them? And he said, nah, we don't have time to focus on all that.

**Steve:** Yeah, I mean, I have to agree with that.

**Leo:** Yeah, we've got other things to worry about. But nevertheless, yeah, absolutely it's illegal. The FBI has been called in. I don't know if they're going to do anything about it. But I just think it's just a really kind of an appalling misuse of their resources for the recording industry to go after, you know, Revision3, a legitimate content company; right?

**Steve:** Yeah, that's not okay.

**Leo:** Yeah. And it wasn't, you know, and this is - as we've talked about before, a real DDoS attack they use raw sockets and other ways to spoof the originating server. They didn't bother. They wanted Revision3 to know where this was coming from. But they had enough servers all over the country that Revision3 couldn't just block a single IP address.

Before we get to the Security Analyzer from Microsoft, do you have any SpinRite tales you'd like to tell?

**Steve:** Well, I had one little reminder. This was a subject, we got a nice note from a Security Now! listener named Dennis Thiel with the subject: "SpinRite Works on Floppy and Saves Wedding." He said, "Steve..."

**Leo:** I'm just dying to hear how this works out.

**Steve:** He said, "Steve, I've been listening to Security Now! from the start. Thanks to you and Leo for a great podcast and great source of information. A while back a friend of mine came to me with a floppy disk that had her address list of guests for her upcoming wedding. She couldn't read it, and desperately needed to retrieve the data."

**Leo:** She didn't have it on a floppy disk, did she?

**Steve:** Yup. That's what he says. "She came to me with a floppy disk that had her address list of guests for her upcoming wedding. She couldn't read it, and desperately needed to retrieve the data since it was her only copy."

**Leo:** What is this, 1979?

**Steve:** This came in on May 9th, so it's recent.

**Leo:** Who has a floppy drive anymore? Wow.

**Steve:** And he says, "I bought my first copy of SpinRite at v5 and have since upgraded to v6. I booted my computer into SpinRite, popped her floppy in the drive, and in just a few minutes it repaired bad sectors and all of her data was recovered."

**Leo:** Wait a minute. You're saying SpinRite works on floppies?

**Steve:** Yeah, it works really well on floppies, actually.

**Leo:** I'll be danged. I didn't know that.

**Steve:** Yeah. And, well, so he says, "Needless to say she was relieved. The floppy drive is all but dead. But I'm sure there are many other people who have data on floppies who don't know that SpinRite will work on them also. Thanks for a great product." And then he says, you know, signed Dennis Thiel.

**Leo:** I didn't know that.

**Steve:** So, yeah, I'm glad you do. Not that you have any floppies on any machines these days.

**Leo:** No, I don't think I could find a floppy disk to save my life, let alone a drive.

**Steve:** I still have them on every single one of my machines. And a little stack of floppies that I, you know, boot for various maintenance and setup and...

**Leo:** Don't you think a CD would be a better choice for that now? I mean, SpinRite will make a boot CD.

**Steve:** Oh, it will. And this guy may well have booted a CD, but then ran it on his A drive, on his floppy drive.

**Leo:** Although you could fit SpinRite on a floppy, can't you.

**Steve:** Oh, no, that always has been. I mean, SpinRite on a floppy, it's like it's 100K or something, so. Yeah, you can put it on a floppy with a whole bunch of other stuff, too.

**Leo:** 100K. Nothing's 100K. I don't even - the text below your name, below the picture is 100K. I don't know how you - that's amazing. Wow, that's so cool. All right. So we talked - was it two weeks ago? - about Secunia's PSI.

**Steve:** Yes. And we had some feedback from people saying, hey, what about Microsoft's Baseline Security Analyzer? It's like, yeah, yeah, yeah, I know, I'm going to get there. And we're going to get there right now. Essentially back when Microsoft decided, sort of woke up from their slumber and said, oh, maybe security is important, remember they launched that whole security initiative, you know, "trustworthy computing" I think was Bill Gates's phrase during one Comdex keynote that year. He says, oh, we're going to be trustworthy and the most secure operating system available, blah blah blah. And it's like, okay, you know, that all sounds good.

Well, some interesting useful things came out of it. These are not things that normal Windows users know about. Using Windows you would never find these offered to you or suggested downloads or anything. So our listeners are going to have to go get them. But both of them I think are interesting and useful in very different ways. The first is the so-called Microsoft Baseline Security Analyzer, or MBSA. And people can use the links in our show notes or on the TWiT page or just go to Microsoft and put MBSA or Baseline Security Analyzer into the little search box, and it'll take you right there. It's not big. It's only a couple meg. And it doesn't have any onerous installation requirements.

The other thing I want to talk about today does require the .NET framework, and that's no longer small. But the Baseline Security Analyzer is not a big deal. And it's very much like what Secunia has done. But it's also impressive because first of all it only deals with Microsoft Windows issues. So it's not a third-party scanner, meaning that it's not a superset of Secunia, nor is Secunia a superset of this. So really...

**Leo:** You could use both.

**Steve:** Well, yes, that's what I would recommend. Both of them together sort of go hand in hand. And when I ran it on a VMware WinXP window that I had where I had deliberately disabled automatic updates about a month ago, after I set it up, I brought it up to current patch level. And I said, okay, now I don't want to be bothered with this. I want to leave this static for a while. I ran it on there. It only takes, you know, a minute or two to do that. And I got severity assessment, severe risk, with a big, red, unhappy shield.

**Leo:** [Mimicking siren]

**Steve:** Exactly. Warning, warning.

**Leo:** Warning, warning.

**Steve:** And it says one or more critical checks failed.

**Leo:** Uh-oh.

**Steve:** And it's like, uh-oh, exactly. And so under security update scan, one of the things it does is it does a comprehensive scan of your system's secure, you know, Microsoft security updates. And it found that one was missing. That got the red shield. And then it also checked for SQL Server security updates to see, well, I don't have SQL Server installed here on this little installation of XP. So that, you know, it came up with a green checkmark because it says none are missing. It's like, yeah, and none are installed, either.

**Leo:** That's interesting.

**Steve:** But very much like the way Secunia allows you to drill down, so does this. So, for example, you can click on what was scanned, for example, when it's saying that it's got my red shield. And then that opens another window which is very comprehensive. And so here it shows me that MS08-028 is a critical update. And it gives me a link. I can click the link, takes me to the knowledge base article. And this was that Jet Database update that we will remember from, like, middle of May, middle of last month. And so it was like, okay, that makes sense that I would have set this up before then and not updated since then.

Then it also - but it goes on and, for example, tells me that I've got three update rollups and/or service packs missing. And so I go, wait a minute, what's that? Well, it's not happy that I'm still using IE6 on this system. So one of the things that it's suggesting is that I update to IE7, Internet Explorer 7 for Windows XP. Number two is the infamous Windows XP Service Pack 3 that I'm not getting anywhere near, although I wouldn't mind sticking it in this virtual machine because this is, you know, just sort of a throwaway scratch VM, so that's not a problem. And then they want an update to, and they always do every month, the Microsoft Windows Malicious Software Removal Tool. So it's saying those things are missing.

Then under the current update compliance I got a whole bunch of green checks. It's basically every security patch from Microsoft that's ever been installed with the number, the severity, and a link to its knowledge base article. So in a way this forms sort of a missing piece of Windows Update/Microsoft Update. And that is it's a nice UI to the whole database that Microsoft is maintaining and that your Windows systems are maintaining, allowing you to sort of have a UI that we don't normally get.

Normally, you know, you get the yellow shield down in the tray. And you go, okay, fine, fix me. And it just goes and does it. And then there is a way in Add/Remove Programs under XP where you can tell a little checkbox up at the top of the window which is normally not checked, you can say "Show my Windows updates." And that of course makes the Add/Remove Programs list triple the length that it was before, depending on how much of your own software you've got installed. Because it'll show you every security update.

But this is just a nicer presentation, and it allows you to see the severity of the patches. And if you have any questions about them there are links for everything that goes around and tells you exactly what it is. So beyond that, though, this looks at - so that's just the Microsoft Windows Update scan results. It also looks, for example, at what they call "administrative vulnerabilities," analyzing the machine that it's on, looking around. And so, for example, I got another big unhappy red shield saying the issue is automatic updates. And so it's just reminding me what I already know, and that is that it says the automatic update system service is not configured to be started as automatic. And it's like, that's right because I'll run it when I want to, not when you tell me I have to. And then I've got sort of a blue eye that says no incomplete software update installations were found. And there's another one, Windows firewall is disabled and has exceptions configured. So that's interesting. I must have turned off the firewall for something...

**Leo:** See, that's good because it's letting you know that you did that. You forgot that you did that.

**Steve:** Exactly. And then I've got - it's happy with me on my user accounts, it says, because it checked my user accounts. And on local account password tests it says no user accounts have simple passwords. So it's checking for password complexity.

**Leo:** Simple being bad.

**Steve:** Simple being bad, yes. Too easy to guess, easy to brute force and so forth. Under file system it says all hard drives {1), so it knows there's only one hard drive here, are using the NTFS file system. So I get props for using NTFS and not having any FAT file system because NTFS, of course, has internal security that allows you to have access constraints on it. Then I get a green check for the guest account. The guest account is disabled on this computer, yay. Then it says this computer is properly restricting anonymous access. So I got a green arrow there. And under administrators, no more than two administrators were found on this computer. Actually I think there's probably only one. I typically, my standard security practice is, as soon as I get a system set up, I delete the account that it forced me to make, and then I rename the administrator account to my own wacky, you know, nobody's ever going to guess this name, so that there isn't even an administrator account named Administrator on the machine, just because, you know, why not. And it goes on. It does basically, I wouldn't say an exhaustively thorough analysis. But there are a couple auto-login and password expiration it skips because this machine - and it explains why, that the computer is not joined to a domain, which is...

**Leo:** Oh, that's interesting. See, on mine it says, you know, you turned on Autolog, because I am on a workgroup.

**Steve:** Ah, okay.

**Leo:** That's interesting, huh.

**Steve:** Yup. And then, you know, it shows, oh, I thought it was interesting, it said some potentially unnecessary services are installed. And it's like, oh, that's, you know, I mean, that's a good thing. Of course Microsoft installed them. So it's like, uh, okay.

**Leo:** Thanks.

**Steve:** Thanks. And then it tells you how many shares you've got because of course over time you might tend to share things and forgot that you left them shared. Gives me a status on IIS, which is their web server, which is available in XP Pro, but I have it either not installed and/or not running. I think it probably installs it by default. But I have it disabled because I went through and turned things off. And the same thing for SQL Server. And finally it looks at IE's zones and tells me that I've got them set up in a way that is making it happy.

**Leo:** Yeah, because you have a very restrictive - on mine it says I don't have any zone settings for some users, and that's a security issue.

**Steve:** Ah, yes. And mine says Internet Explorer zones have secure settings for all users. So anyway, I wanted to bring this to our, obviously to our users', to our listeners' attention because it's free, it's not big, it's easy to run, and it's just, you know, one more useful check on things that, you know, again, like for example, you know, the firewall turned off, you left some shares on some folders that you no longer need, you turned on your guest account and you forgot to disable it even though you don't need it anymore. So it's just a simple, easy way of sort of, you know, taking a little check on your machine, just sort of doing a little bit of an audit.

**Leo:** So this is free. It's from - if you Google MBSA, that's a quick way to find it. It's the first thing that shows up. And while you were talking I downloaded it and ran it, and it did, it pinpointed a number of things. It even suggests, you know, it says click here to find out how to fix that, which is great.

**Steve:** Yeah, and again, it gives you - I really like that it gives you essentially a user interface into Windows Update. Because so it's not just - it's no longer just, okay, I don't know what's going on, just go ahead and fix things, it allows - especially now that I'm, like, being reticent, well, actually I'm more than reticent to put Service Pack 3 on my machines after it hurt two of them. So of like, uh, no, thank you. So I just - I like the idea that there is a user interface to that.

**Leo:** Yeah.

**Steve:** So that's the first of the two things. The second one is very different. They call it the Microsoft Security Assessment Tool. And I sort of, as I was refamiliarizing myself with it, I thought, you know, this is a little bit like therapy. This is like security therapy because it doesn't tell you what to do, whereas the Baseline Security Analyzer certainly does. It basically asks you a bunch of questions. And so the idea is, I mean...

**Leo:** It is like therapy, isn't it.

**Steve:** It's just like therapy.

**Leo:** How do you feel about this now?

**Steve:** And so, you know, it wants my company name, and I put in Gibson Research Corporation. Number of desktops and laptops in use at your company.

**Leo:** Wow, that's interesting. Wow.

**Steve:** I said fewer than 50. Number of servers in use at your company, and I said one to five. And so that's like the first page. And then it just basically takes you through the next status, is what they call a "business risk profile." Does your company maintain a full-time connection to the Internet? And so you've got, for all of these, yes, no, and I don't know.

**Leo:** I got no idea.

**Steve:** And there's oftentimes a little question mark icon at the side. And then, like, if you're not really sure, it'll say, like, such as a T1 or a DSL line, cable modem, or other always-on connection. And so you say okay, yes. Do customers and vendors access your network or internal systems via the Internet? So customer and vendors access your network or internal systems via the Internet. And so it's like, well, yeah, we've got a website, for example.

**Leo:** Oh, yeah, of course, yeah.

**Steve:** Does your company host application services such as a portal or a website or external customers or partners? Yes. And so you click that. And so, for example, for that question, if I float over the little question mark it says, if you are hosting application services for customers or partners, there is an increased risk to the infrastructure due to the potential for data loss or threat or service unavailability. So basically, I mean, and this is just the tip of the iceberg, this thing, you know, I spent, god, an hour with it. And, I mean, the reason I call it therapy, and the reason I think it's a useful thing for our listeners, for Security Now! listeners, is in the same way that a therapist asks you questions that are, like, leading questions that cause you to think about yourself in a way you didn't by yourself, similarly this, you know, it asks you questions about how was your network segmented, do you use a VPN...

**Leo:** Now, does it make recommendations based on all this, or is it, like, just trying to get information about your system?

**Steve:** No, no, if you finally - if you make it through this whole thing - and so there's like a first pass where you sort of characterize yourself. Then based on the first pass answers it goes into the next level, which because now it knows enough about, like, the way your network and your company or your home, I don't mean to say that this is only of use for IT sort of people, anybody who's got a network at home could, I think, find these questions very interesting because in answering the question you kind of think, oh, I mean, it asks you about, like, do you use a router with a DMZ? And so you basically go through a first pass where it gets a sense for who you are. Then based on that collection of answers it goes into, like, it drills down to a next level of real detail about how your system is configured. And when you're finally done, it gives you a report card. It literally tells you, okay, here's the things that you're doing that you need to worry about. These are areas where you really, you know, your policies need review. I mean, and it asks you things like do you have an enforced password policy that requires you to change passwords periodically? Now, of course, as with a therapist, you can say, uh, yes...

**Leo:** I'd prefer not to talk about that if you don't mind.

**Steve:** Nobody's making you tell the truth. You can lie to your therapist. You can lie to Microsoft's Security Assessment Tool and tell it, oh, no, I never go to those naughty sites. But if you tell it the truth, I mean, just the act of filling this questionnaire out I think is really illuminating and useful because, although I have to say most of what I found on myself being asking [sic], I was pleased to see that in our coming up on three years, we've covered everything. I mean, it even...

**Leo:** Oh, that's interesting.

**Steve:** It even goes through, if you tell it yes, like does your organization use wireless, yes, then you get a whole expanded box of, okay, which security protocols are you using? And they're all there. WPA, WEP, we run an open network block, but, you know, ooh, you don't want to even think about checking that one and seeing what it's going to do, it'll probably just melt down. But it's - I think it's something that our users, our listeners will find really worthwhile. Now, the downside is this thing requires .NET v2, which in itself is only...

**Leo:** So this isn't just an online survey, which it, by the way, could easily be. I mean...

**Steve:** That's a very good point.

**Leo:** ...this could just be a questionnaire online. You don't really need to download - but you do, you have to download something. And you have to have .NET installed.

**Steve:** You have to have .NET installed. Now, you know, Microsoft's pushing .NET. I know there are people who are deliberately staying .NET free. Long-term I think those people are going to lose because essentially .NET is the next-generation API for Windows. And more and more things are requiring that .NET be there. So...

**Leo:** It doesn't hurt to download it. If you've got Vista, you've already got .NET.

**Steve:** Precisely. Well, that's a perfect example. And this is why I set it up in a VM. It was just like, I'm going to resist .NET till the bitter end, until I really need something on my main system that requires .NET. And maybe by then they'll have, you know, we'll be at Service Pack 9 on .NET, and it'll actually be stable and not a big security problem. Because again, like anything else that's new, Microsoft has had security problems with .NET. So I just - I work not to put junk on my machine that I can avoid putting on. So I installed .NET in a VM, and I ran this in a VM, knowing that I'd be able to...

**Leo:** This cracks me up. It's 12.5MB. I mean, you just talked about SpinRite, which is so incredibly useful, is 100K.

**Steve:** Yeah, I ought to get the right size for that. It's actually...

**Leo:** I think it's more like 90K.

**Steve:** No, no, no. It used to be 96. That I, well, it used to be 64, used to fit into a COM file.

**Leo:** Then it got a little too big, yeah, yeah. Well, all I can say is 12MB for basically what is a questionnaire is absurd. I'm running it right now.

**Steve:** Okay, 169K is SpinRite.

**Leo:** 169K. So this is like, what is it, a thousand times bigger.

**Steve:** Now, yes, not so - well, okay. The actual Security Assessment Tool is 12.5MB. .NET, however, is really big. I think it's maybe up to like 68MB, something like that. You know, it keeps growing. They're now at 3.5 is the most recent one, which is the one that I installed. But anyway, I wanted to bring both of these tools to our listeners' attention. I think certainly the Baseline Security Analyzer, it's just nice to have it there. It's small and lightweight. I think it's 1.5MB. Easy to run. And again, it's just another little check on making sure that there's nothing obvious that you've forgotten, and as a really nice user interface into Microsoft Update and all of the endless, you know, the patch stream that we've got. And then secondly, you know, this security therapist, the Security Assessment Tool...

**Leo:** It's ELIZA. It's ELIZA for security.

**Steve:** Well, except that this is just - well, yeah, I guess that's a good point because it's not quite as interactive as ELIZA was back in the day. But what it takes you through is useful. I mean, don't be in a hurry. Just think about the questions. Like do external partners or customers connect directly to your company's internal backend systems for the purpose of data access, record updates, or other information manipulation? You know, it talks about what do you subcontract out? What services do you get from the outside? I mean, it really builds a threat and risk model based on these questions.

**Leo:** And I could say this looks more like - this survey looks more like a marketing survey than anything else. I'm giving Microsoft a lot of information about what I do.

**Steve:** Well, yes. And I was a little skeptical. I did skip that whole first fill out about - everything about your company and all that stuff. You're able to skip right over that, and you don't need to fill that in. And I was, as I was going through these questions, I was skeptical about are they spinning this in a pro-marketing, pro-Microsoft way. And I have to say no because there were several places where the advice that I was being given was not pro-Microsoft.

**Leo:** Well, that's good.

**Steve:** Yeah. I thought it was, oh, I love "Does your company share office space with other organizations?" You know, again, it's just...

**Leo:** Yeah. Well, that's legitimate, that's a legitimate thing to ask because...

**Steve:** Oh, no, that's...

**Leo:** ...that means other people had physical access to your systems, and that's relevant, yeah.

**Steve:** Yes. No, I think this is all legitimate to ask. And again, I recommend this for our listeners. I think, while a lot of it is more corporate oriented, it's also, okay, like - or, well, do you have roommates? You know, that's the same sort of question.

**Leo:** Right, right.

**Steve:** Brought down to a home level. Does your roommate have access to your machine when you're not around? So, I mean, it's these are questions that are really worth thinking about once. And then you can just drop them, never think about it again. But it'll push people to think about, oh, I know what the right answer is, but ooh, mine is not the right answer.

**Leo:** Right. Well, that's an important point, yeah. All right, Steve. A couple of - we'll put links to both of them, although it's easy enough to find them if you just look for Microsoft security tools on Google or your favorite search engine, your search engine of choice. It's not hard to find. But we will put links in the show notes to all of this.

Steve, you're at GRC.com, and I know that's a great place to go if you are a fan of the show because you'll find a variety of things there, including the 16KB versions of this show. So if you've got not a lot of bandwidth and you want to download the show, or maybe a friend's on dialup who would like to get it, or you just want to put it on a floppy - would it fit on a floppy? Probably not. It might. It might. Go to GRC.com. While you're there you'll see transcripts. Lot of people like to follow along as Steve's speaking because frankly this is, as they were saying in the chatroom earlier today, an information-rich podcast. There's more in this podcast per square inch than any other show on the Internet, including all of my shows. So the transcripts help a lot. We thank Elaine for making those transcripts. And you can get them, and show notes, and links at GRC.com.

While you're there, don't forget to check out all of Steve's free security programs - ShieldsUP!, Shoot The Messenger, DCOMbobulator, Unplug N' Pray - he's really good at names. And of course his bread and butter and the program we recommend every program is SpinRite, the world's finest hard drive maintenance and recovery utility. Somebody in the chatroom asked can I use it on my solid state drive.

**Steve:** You do not want to use it on your solid state drives. The technology is all about magnetic medium. And a solid state drive is, as we've discussed on this show, is definitely sensitive to read and write cycles. So there's no need for it because the kinds of actual physical recovery that it performs does not map onto solid state memory. And it's bad for a solid state drive because you do not want to write, unless you need to, to a solid state drive.

**Leo:** Yes. So don't mess with your SSDs with Security Now!. But if you've got a hard drive or a floppy, would it work - it would work on ZIPs, then, I guess, huh?

**Steve:** In fact it was v5.0's support for ZIP which started the whole "click of death" deal is we started, as soon as v5 came out of SpinRite, which for the first time supported ZIP and JAZ drives, those two Iomega technology drives, people were saying, hey, this is a cure for click death, it cured my click death. And I said, it cured your what?

**Leo:** What is that?

**Steve:** And it turned out that SpinRite actually, similar to it on Flash drives, you did not want to run SpinRite on a drive that had the so-called "click of death." And that's why I wrote the free tool, Trouble In Paradise. Which again, as I guess you probably - I think you did like the name of that one, as well.

**Leo:** TIP. Because it was TIP.

**Steve:** TIP, Trouble In Paradise, which was a free gizmo for Iomega users that properly assessed the status of their drives. And we told people, no, don't run SpinRite on them, it'll just make a bad problem worse.

**Leo:** And in fact that was how we first met was talking about the click of death and TIP, Trouble In Paradise, many moons ago now, Steve Gibson.

**Steve:** Many good moons.

**Leo:** All right. We're going to wrap this thing up. Again, GRC.com for show notes and transcripts. And we'll be back next Thursday and every Thursday for another episode of Security Now!. Thanks, Steve Gibson.

**Steve:** Talk to you then, Leo.