

Book Review: Thor's Microsoft Security Bible

Review by John R. Luko, Security+, CCENT, CEH

A few weeks ago I saw an ad for Thor's Microsoft Security Bible: A Collection of Practical Security Techniques (TMSB) by Timothy "Thor" Mullen and thought, "Hey that sounds like it could be useful." I work for a Managed Services Provider (MSP) that supports tons of Microsoft servers, so any extra knowledge can always come in handy. Originally, I thought it might be over my head. I held off on buying it, until I found some reviews. Fortunately (or unfortunately depending on how you look at it) TMSB came out and no reviews have been found. I decided to go on Amazon and read the first chapter for free to see if it was something I could handle. After reading the intro and half of chapter one, I was hooked.

Before I get to the review and some thoughts, I thought I'd offer a couple quick hints. The first hint is to buy the hard copy. Online retailers are selling the electronic version for the same price as the hard copy, and there is media that comes with the book. Therefore, getting the hard copy gets you both for the same price. Second, having read through the book, I'd suggest having the following intermediate level skills: C#, T-SQL, and Server 2008 experience. On with the review!

Discuss in Forums {mos_smf_discuss:Book Reviews}

Introduction

The introduction for TMSB by Timothy "Thor" Mullen (pictured right) is one of the best I have read of any security related books. First, the author explains that he is going to convey the information with a first person style of writing. He keeps true to his word making reading through the short 298-page book (not including appendixes) very quick, as I felt we were almost having a conversation. Second, the author speaks to three ideas that really struck a chord with me.

1. Feasibility of a hack – sure there is a way, but what is the likelihood of people actually doing it.
2. Motivation behind releasing holes found – less to improve security, more to improve ego/stature.
3. Looking at things from a defensive angle – this could be debated, of course, but you do see more and more that everyone is thinking offensively.

I highly recommend that, even if you don't purchase the book, to read the introduction for free on Amazon. It is eye opening to say the least. On a final note in regards to the intro, the author focuses on two security domains that he feels remains the same in almost two decades of working in security: least privilege and security in-depth. You'll find these two ideas to be the themes throughout the book.

Chapter 1 - Securely Writing Web Proxy Log Data to SQL Server and Programmatically Monitoring Web Traffic Data in Order to Automatically Inject Allow/Deny Rules into TMG

Boy is that a mouth full. The first chapter covers using Threat Management Gateway (TMG) to monitor the sites that people are visiting, and write it to an SQL database. On top of that, when the users go somewhere they should not, it adds them to a group that prevents them from accessing any other websites (on top of making fun of them for trying to get to a denied site). When I initially saw this chapter, I thought, "Isn't this supposed to be a security bible? Where is the change this setting and turn off this service?" You'll find that the author is teaching through example and while you might not ever implement this system for monitoring web traffic, you can certainly use pieces of this project for other activities that could arise.

Throughout the chapter the author basically walks you step-by-step through the various settings for the security group, SQL, TMG, etc. There are included screenshots and code for everything the author does. Remember the media we spoke about? Well source code is found on it as well as two videos, which I will discuss later. Thor covers securing the data in transit, securing the user with least privilege (allowing it only to add/remove to the security group setup), and near real-time analysis of the logs to auto add users to the group when they go where they shouldn't.

I really enjoyed the chapter, but there were a couple of issues. First, I believe this should not have been the first chapter. Thor points out that you should read chapter 5 when he begins discussing setting up the user. I would assume we could have made that the first chapter, if you will reference looking at it. Second, for the log analysis he states near real-time (basically a process will analyze the logs every 2 minutes). Somehow giving a user two minutes to continue what they are doing doesn't sit well with me. But there were some great aspects to it as well. The author's humor makes a topic that could have been dull, very enjoyable to read. He also goes through three ways of dealing with having SQL analyze the logs and add a user to the denied group. He addresses issues with each, from worst to best, and explains his reasoning. Finally, I loved that he discussed securing the data in transit. This isn't always something people consider, but it is a great idea (maybe not for blocking web traffic, but practice like you play!).

Chapter 2 - Internet Information Server Authentication and Authorization Models, and Locking Down File Access with EFS and WebDAV

In Chapter 2 the author discusses using a web server to allow users to access files on another server (internally) from anywhere (externally). He takes it a step further by discussing how to setup a mapped drive using http securely (instead of connecting to a VPN), which I really enjoyed. Thor discusses a number of different technologies in this chapter, but I really enjoyed his coverage of Windows Encrypting File System (EFS). This is a feature that I feel is under-utilized, which is a shame. Playing to the security in-depth side of the house, he walks through various features (EFS, least privilege settings, and encryption of traffic) to give an attacker various layers to work through. He ultimately ends with the data being encrypted and the users not being able to view it if they wanted to.

I can honestly say that there was only one thing I didn't like about this chapter, and it was that the author does a thorough job of scaring you from wanting to use EFS. Let me explain. Thor warns you with a story about what could happen if EFS isn't setup properly. He goes through how it works (a great overview and explains that you should definitely look further into it), and then tells you how things can go wrong. After reading what could go wrong, I wasn't too thrilled at the thought of trying to set it up in a production environment. I felt this might work against the author, but you can at least say he is just trying to warn you. Again, the author's humor was great, and I really did find this chapter to be very interesting. Also, to see a great overview on not only EFS, but RSA encryption (that is easy to understand) was a huge plus for this chapter. The coverage of key encryption was one of the best I have read. Finally, I liked that he built off of the first chapter and chapter 5 (yet another reason why chapter 5 should have been first).

Chapter 3 - Analyzing and Blocking Malicious Traffic Based on Geolocation

This chapter title was pretty self-explanatory. Thor discusses blocking traffic based off the country from which it originated. This is something that even the author will admit, could be an issue setting up on a network. He doesn't know your business and states clearly that a lot of research should be done prior to deploying a solution of this type. That being said, having the ability could be a nice weapon to have on hand, even if you don't turn it on until needed. Thor also sites places used for research which is great for the reader.

My main issue with this chapter was really the amount of work that would go into setting it up. It appears that TMG does not store IPs in octet format, and the only way to convert it is with a little code. Now for someone who works with it on a daily basis, this could be no big deal. Also, you could easily go out and find the code already completed for you. I have trust issues, so I am not a huge fan of that idea. However, there is an article in the MSDN that has the code, so you are covered from that point. There are two shining points in this chapter through. One, the author gives an excellent editorial on security policies for developers. His ultimate point is that you cannot simply tell your users what they can't use (in this `sp_executesql`) without giving them a viable alternative. Thor points out that more than likely they will attempt another solution that would just open a hole just about the same as the one found in `sp_executesql`. Two, I do like the

idea of being able to block traffic based off of location. In the MSP environment, we do have companies/small businesses like Doctor's offices that would not receive traffic from outside the US (perhaps even the state, but I wouldn't make a blanket statement such as that). It's always nice to have options if the need arises.

Chapter 4 - Creating an Externally Accessible Authenticated Proxy in a Secure Manner

This chapter works to setup a proxy that users on the outside can use to browse the web while appearing to come from inside the network. Thor's example speaks to allowing a friend to view programming that only those with a US based IP can see. We can skip the legality of this and just focus on the setup. Setting this up was something that I felt should definitely be done for the road warriors at an organization with company provided laptops. Combine it with setting up a mapped drive through http (as discussed in Chapter 2), and you have a one-two punch of awesomeness.

At this point, this was one of my favorite chapters. Thor goes as far as to discuss how to segment this traffic from the LAN, which plays into his security in-depth model. I had nothing bad to say about this chapter, and that could be because I found it applicable to my job (plus it was fairly cool all around). He covers a fair amount of topics from Hyper-V to port redirection. An interesting point he made was about security through obscurity. Like most of you (I make an assumption here), we've always heard that security through obscurity isn't security. But Thor makes a valid point in that it can be security to a degree. The short and sweet of it is, it can be another layer of security (like an onion) albeit quickly uncovered. His example was having the user input 52011 as their port for the proxy and this forward to 8080. This in turn would require an attacker to scan the entire port range. So while they would probably quickly realize what was up, they'd still waste some time.

Chapter 5 - The Creation and Maintenance of Low-Privileged Service Users (with a Focus on SQL)

Finally, we reach the elusive Chapter 5. This chapter became my favorite chapter as it played a little more to the security bible title. Least privilege is a major topic and is very important when you look at security in-depth. Thor specifically speaks on this topic in an example of setting up MS SQL Server with a Service User account. He discusses how if the job only requires them to do two things, why give more access than is needed? More to the point, by doing this you can implement a number of GPOs on the group setup for these accounts (such as password policy and a lockout policy) that they otherwise would not get. Thor even speaks to taking it a step further and through log analysis locking the account if it gets compromised and attempts to access resources it has no business accessing.

My only gripe about this chapter? You got it, should have been chapter one. Can you tell this hit a nerve for me? If I ever get a chance to meet the author (highly doubt that would happen), I would shake his hand and then attempt to get the reasoning for this being Chapter 5. Again the walkthroughs in this chapter were great and the author points out when you should look to another resource to go deeper. Obviously, the book cannot cover everything, and it's nice to see an author who acknowledges this fact. The other interesting topic covered in this chapter was the author's idea of true password complexity. I dare not try to truly explain it, so I will leave it as it is very interesting, thought provoking, and if you decide to purchase should be read ASAP.

Chapter 6 - Remote Security Log Collection in a Least Privilege Environment

In Chapter 6 we cover remotely pulling the security logs from a server and placing those events into an SQL database. There is a ton of code for this chapter, so hopefully you have knowledge of T-SQL and C# (or some vague knowledge so you can follow it). The author makes use of RPC and the WMI for pulling his data. He sets up a secure method of connecting using authentication and then encrypts the data in transmission. This chapter builds off of the previous chapters, so a thorough understanding of the concepts covered to this point is needed.

This was a great chapter, but it is very code heavy. A lot of the pages in the chapter were code that the author wanted you to look at. Perhaps he was trying to get the page count of the book up, since he included the source on the DVD, and you could read that at any point. It was very interesting to see the uses of WMI, as from an MSP standpoint we use this for the monitoring of our servers. I do find the chapters that I can apply to what I do on a daily basis are the best and this chapter does get the ideas flowing. Be prepared for a depth of knowledge into the Windows Server 2008 OS!

Chapter 7 - Securing RDP

A chapter with a short title? Yes, I was just as shocked when I read it. In Chapter 7 the author walks through how to secure RDP. He starts off by explaining the various iterations of the naming of RDP, then covers the changes made to make it more secure. He actually answered a question I had in regards to the changes on 2008 Server vs 2003 Server. Thor provides several methods for securing access to the RDP from the Internet and provides a custom program for designating the source port. This chapter wasn't as heavy in the code as Chapter 6, though he did take up a number of pages for the code itself.

This chapter is probably the most applicable to most Windows environments. Thor discusses his overall theory on RDP and DMZ setups in general, which I believe had many valid points. He offers several options for using RDP and all in a secure matter. Also, he explains how RDP works in general and the common misconceptions in its security. Again, security through obscurity is discussed, and I can side with the author's opinion on RDP. He also went so far as to cite some data run from a personal experiment that he performed. Obviously, not knowing all the factors we cannot give official credence to the study, but you can get the general idea and form your own conclusion.

Final Thoughts

Having completed the book I can honestly say that the only problems I had were really not with the content per say. I would have preferred that Chapter 5 be Chapter 1, as it would have been a better starting point. Including the code samples in the text itself when they are on the DVD, made it feel like just page filler. There were a lot of screenshots, which isn't a bad thing, but I felt as though the placement could have been better thought out. In basically every chapter you had to jump ahead a few pages to see what the author was referencing and that can get confusing. Also, the placement of the included DVD was not correct. Generally, I am use to looking to the back of the book for the media and didn't find it initially. I flipped through the pages and found it was in the middle, which didn't make a whole lot of sense to me. Finally, I didn't understand why there was no general conclusion written for the book. You have a solid introduction, great content, but then there's the odd choice in just ending the book at Chapter 7. Perhaps I am being picky, but I was looking for a conclusion to give me that warm and fuzzy feeling. It's like a movie that abruptly ended about 5 minutes before the credits. It didn't take away from the story it was telling, it just felt disjointed.

Obviously, most of my issues are basically cosmetic. Earlier in my review, I said I was looking for the standard security bible (change this setting or that setting), and I did ultimately get that. Thor's chosen delivery method does walk through the changing of settings, but does it in such a subtle way as to not make the content boring. This is a book that when you begin, you think "huh?" But once you complete it, you think "Ah ha!" Generally, security bibles can be dull, but given the author's humor, vast knowledge of securing Windows Server 2008, and his ability to explain the topics to even a novice, makes this work shine. Anyone working in a Windows Server environment is doing themselves a disservice by not reading this book. The included video content was refreshing, as the author continues his dialogue with you. He walks through setting up Chapter 1 and Chapter 7 on the fly, so any mistakes you will see. It was nice to hear his voice, since, if you're like me, it makes it easier when reading. TMSB is a great book, and for all you Windows 2008 Server Administrators out there, I'd run, not walk, to get this book!

John R. Luko, Security+, CCENT, CEH

Mr. Luko graduated from Drexel University with a BS in Computing and Security Technology with a concentration in Computing Security in Dec of 2008. He began working as an IT Tech for a chemical company, where he did everything from server administration to troubleshooting and advising management on security concerns as they arose. From there he left for a position at a managed service provider. He is currently a NOC Analyst/Helpdesk engineer, where he does a little a bit of everything. He is also charged with validating PCI Compliance Audits performed by third parties and remediating any issues.