

**Vulnerability  
Management  
and  
Penetration  
Testing**

**SANS WhatWorks  
in Internet Security**

**CORE IMPACT  
at the  
Commonwealth  
of Pennsylvania**

2007



## *Securing Networks from Malicious Code and Attacks at the Commonwealth of Pennsylvania*

### About Robert Maley

Robert Maley joined the Commonwealth of Pennsylvania in July 2005 as an IT Consultant managing the Enterprise Security Auditing and Monitoring project, a component of Operation Secure Enterprise. He joined Enterprise Architecture as the first Chief Information Security Officer for the Commonwealth in November, 2005. His day to day responsibilities include information security architecture, policy compliance and strategy for the Commonwealth's enterprise infrastructure and the 47 agencies, councils and commissions that fall under the Governor's jurisdiction.

### About the Commonwealth of Pennsylvania

The Commonwealth of Pennsylvania occupies 44,800 square miles and has a population of approximately 12,400,000. The State's Cyber Security Information Security Office provides a website offering best practice guidelines and other awareness materials.

### SANS Summary

Significant interruptions from virus outbreaks in its systems caused the Commonwealth of Pennsylvania to invest in a penetration testing tool to supplement its technical controls. The tool selected allowed the security team to take existing knowledge and leverage it through automation to accomplish a lot more in a shorter period of time.

-----

### *Interview*

Q. Tell us a little bit about the job. You're the CISO for the State of Pennsylvania, right?

A. Yes. The position was created about three years ago with a program they got started called Operation Secure Enterprise, which was the response to some significant interruptions the Commonwealth had several years ago, around 2003, due to virus outbreaks. They decided to fill it in the last half of 2005 and I was appointed December, 2005.

Q. What triggered the move to a penetration testing technology?

A. I looked at the overarching strategy that the Commonwealth had for enterprise security and I found that it was very heavily weighted towards implementing technical controls. There really wasn't any strategy toward vulnerability scanning, pen testing or

-----

*\*To hear Robert Maley expand on the answers, view his presentation slides, and listen to his answers to many more detailed questions asked by other users from around the world, go to <http://www.sans.org/webcasts/archive.php>.*

***“Core Impact gave my security guy the ability to ... .accomplish a lot more in a shorter period of time.”***

risk analysis. That was all just kind of left out in the ether; nobody was looking at that and when I developed a strategy that we’re now in the process of implementing, that was obviously a component of it. One of the areas I found very difficult for things to happen, in our state at least, was funding

for small agencies. Pen testing is something that requires expertise. Even though you have an automated program, there still has to be expertise behind it. Somebody needs to know exactly what they’re doing and why they’re doing it, and small agencies didn’t really have the need to have somebody full-time to do that. They didn’t have the resources to buy the software that they would need to do that. So that was one of the areas that fell into a bucket that we call tiered services. We’re trying to develop a menu of shared security services for those agencies that they can’t fund or don’t have the expertise to do themselves. So that’s really what drove us to add penetration testing as one of those services.

Even if you’re smart enough to turn it on and it works, you may not know what the results that it gives you mean if you’re not experienced.

Q. You said that you needed to do penetration testing because that was a weakness across all agencies. So how did you go about choosing a tool?

A. I have a very highly capable staff; some of the individuals have some pen testing experience so they went out and they just looked at different products.

We have different processes we have to follow in the Commonwealth depending upon the dollar amounts for the products. At the time, the funding I had for this particular component was limited and it fell under the limit that would require us to go out and do an RFP or an RFI. So we reviewed all the different products that were available and my lead security guy made the decision on which one to use.

Q. Do you remember any particular characteristic of this technology that just made it, “Oh yeah, that’s the one we really do need”?

A. The automation, because my security guy has the ability to do everything the product does, but on a very time-consuming basis. And the product gave him the ability to take his knowledge and leverage it through automation and accomplish a lot more in a shorter period of time.

Q. What was the process of implementation? How long did it take? What did you have to do?

A. It took about a day. The software got here and my expert got it up and running. I think that it was about two weeks later when we had a training session via web conference; he pretty much understood the product at that point, but had some

questions. At that point we were up and running; we had the service available to agencies. Implementation went very smoothly.

Q. So now you've got it running, what proved to you that the investment you made would actually improve security?

A. I don't think it actually improved security as much as it shows that certain processes and programs that we have in place are working. As with any state government, we're the repository of a significant amount of information on our citizens. The number one priority in any government service is to make government easier, but in that process, we have to ensure that all those little pieces of security information remain secure. Therefore, we've developed processes for security assessments and vulnerability scans—and they're all good—but we also go in after remediation and use it as our tool to check our work.

Q. Can you honestly say you didn't find anything that didn't work?

A. We found some holes that people missed in the remediation and we were able to then remediate those issues. In that one case alone, the value we got back far exceeds what we spent.

Q. That makes sense. I thought you were saying that it just validated that everything was right and I don't know anybody that has that environment.

A. I wish we validated that everything was right, but no. It points out areas that we missed and it's just another level that we use. My theory is that the more levels we have of compliance checking and of secured systems, the better it's going to be because we can never be 100% secure.

Q. So you're seeing it as part of the client structure? Demonstrating to the legislature, demonstrating to the auditors that you really do validate your systems and identify and fix weaknesses?

A. Correct.

Q. What kinds of problems did it find?

A. Typically configuration areas or missing patches.

Q. So a configuration area might be a password problem or a service turned on that shouldn't have been?

A. Right.

Q. Couldn't you have used a vulnerability tester rather than using a penetration tester?

A. We actually do that as a first pass in the process and we feed the results of the vulnerability scan into the tool, because obviously the number of assets that we have is

**“We found some holes that people missed in the remediation. In that one case alone, the value we got back far exceeds what we spent.”**

significant, and for us to be able to do this on every asset that is under our jurisdiction is impossible—we would need a much larger staff. Consequently, we do our first runs with vulnerability scanning, which can generate a lot of false positives, and then we use the pen testing tool to verify it.

***“Tech support is very good... a lot of times I call (them) to actively try to exploit a system with that vulnerability listed on the exploit itself.”***

Q. But how does this system show you what the vulnerability tool is missing?

A. I don't think there's any one security technology or security tool that's going to catch 100% of vulnerabilities, just like I don't believe there's any antivirus program out there that will catch 100% of

viruses and Trojans. So having one product at one level and a second at another level is good security practice.

Q. How do you use it? Does it run all the time in the background? Do you run it once a day against one agency and another day against another?

A. The first thing we've done is to make agencies aware of the service, and if they determine that they have a need for it, we will respond to that. An example is an agency that has an application that contains some significantly sensitive data and underwent a third party security assessment. They wanted to be assured that the company that did the assessment did a good job. We went in and had an engagement with that agency on the server to ensure that a) the third party did a good job on identifying problems and b) that the agency did a good job on fixing them. In that case, it turned out positive that both the third party and the agency did good work and we just confirmed that the work was done well.

Q. And does the agency put some money into the pot when you do this service for them?

A. Not yet. Right now it's a free service to agencies.

Q. Can you describe these "engagements"?

A. It's probably about a one week STD total. We have a meeting where the rules of engagement are hammered out. It's a very extensive document that we make the agency fill out so that in our processes, we make sure that we don't take down any services that are critical at a time where it would affect e-government to our citizens. So all the rules of engagement are very clear on what they want us to do, where they want us to do it, and when we're going to do it. And then the second step is obviously that we schedule it and we have someone go out and do it. Typically it's about a week's worth of effort involved.

Q. Were there any interesting rules that you learned along the way? Was there anything that wasn't obvious in the beginning that you added because you learned you needed it?

A. I think we did a pretty comprehensive job up front, and I don't think there's anything significant that we ran into. We're very cognizant of the nature of the types of services that we have. We pretty much built in those timeframes and black-out periods; we have a checklist that we go through to make sure the agency understands all those things.

Q. So then how many hours a week or month would you say you're using this technology?

A. Well, that varies. It depends on agency demand. We don't have anybody that's full time doing it, but I would estimate maybe a week a month.

Q. Has any other state followed you, followed your lead on this?

A. Not that I know of. We really haven't had a chance to talk about it. I remember hearing an attorney general someplace is doing it.

Q. How has technical support been? When have you needed it? How responsive has it been?

A. They've been very good.

Q. Do you remember what you had to ask them about?

A. A lot of times I call tech support, not necessarily for operational reasons, but I'd say once every two weeks they have active exploits that are imported into the program. I want to know how they work so we can utilize them. Therefore, a lot of times I call tech support to actively try to exploit a system with that vulnerability listed on the exploit itself. So even though it's imported into the system, you don't necessarily know how to use it.

***"I love the client side exploit and the remote side exploit."***

It's not just cookie cutter where you just point and click and go. Sometimes— actually, a lot of times— you have to be creative about getting the exploits on the machine itself. So it's not just point and click and move it over; there is a little work involved and some creativity in using a hacker mentality and putting that exploit on the machine. They have some tips and tricks on how to actively apply some exploits over others and that's why I call tech support.

Q. You talk about using a little creativity in getting an exploit on the box. Give us an example of what you might have had to do to get something on the box. What did you have to do?

A. Sometimes there's an active exploit, say an Internet Explorer exploit, which is on the client side and is not normally done from a remote site. In other words, I need to have a

user interaction to exploit the machine or exploit the vulnerability. One defense might be to tell your users not to click on this link, or not to click on emails that aren't familiar to them. So you need to set up an email server, of course, to have some way of getting an email to a certain user on a system along with a lot of client side exploits, and have a user do something on their end to actually exploit a client side exploit. For example, I could know that there is a Joe Smith or Sue Johnson in the Commonwealth, send an email there and just wait for that user to click on the link and then toss back to my remote server that would be listening on it.

***“A positive was how easily it could be used... and they do have some risk features that show what's actually happening.”***

I'm just hoping that somebody does something that they're not supposed to do because the agent would then be installed on their machine and then I could actually own the machine, but if the user doesn't do anything on the client side, the exploit won't happen.

I love the client side exploit and the remote side exploit. And if you don't call CORE IMPACT, a lot of times you don't know how to exploit the client side. Every time we get a product release, and we've been running it now for two years, they tell me I should really call up for info about the latest client side exploits and how to use them.

Q. Did you find anything that was a little surprising? You knew it would work and you had some expertise before you started, but was there anything once you got it that was a little surprising to you, either positively or negatively?

A. The positive was how easily it could be used. Another positive is they do have some risk features on the tool that show what's actually happening. They do enable that. Concerning some of the negatives that I've seen- not the false positives, but simply a lot of time exploits won't work when fingerprinting an operating system -- you can't exploit a machine if CORE IMPACT doesn't have a vulnerability to work with. So sometimes I use another external scanner such as ISS or DFI LAN Guard. As the end user, I didn't realize that until I did a little research on my own and realized oh, okay, there's no exploit for that, so CORE IMPACT won't be able to do anything.

Q. Does the fact that there's no exploit in CORE IMPACT give you confidence that the bad guys can't exploit it either, or not so much so?

A. Not so much, no, not at all. Actually, I've used Metasploit as well- though I can't use both of them at the same time because that would take a little effort to get up to speed with Metasploit. Working with both of the products at the same time is highly advantageous because a lot of times Metasploit takes a little bit longer than CORE IMPACT and vice versa. One might be faster than the other to exploit.

Q. And that's another reason why you want to have experts running the tool, not just anybody running it?

A. Exactly. A lot of times we give it to a vulnerability person who runs vulnerability scans like Nessus scans or GFI scans; it's a different beast, it's a different animal, it's an enhancement. You can use it as a point and click and walk away, but you're definitely going to miss a lot. I run it and I sit with the tool to see what's actually happening, and many times, I hammer one type of vulnerability with many different types of exploits.

Q. You talked about how tight the budget is. How exactly did you go about getting the funding for it? Was there any special trick you used, any special selling point?

A. With the implementation of Operation Security Enterprise there had been funds that we didn't use because we did it very well, very quickly and under budget--that left dollars there that we could use for these additional tools.

Q. Are there any additional features you wish it had?

A. It's not so much a feature, but I've already told CORE IMPACT that I'd like them to offer Web accessible sessions for the latest exploits--maybe a monthly update. Their engineers are very, very sharp, and very, very savvy. They know the tool better than anyone else and they know how to use client side or remote exploits better than anybody, but the documentation won't help you with that. CORE IMPACT created movies of screen captures, presentations, telephone presentations and walkthroughs, similar to online training, of how to run some of the latest client side exploits and remote exploits and that's been very helpful.

Q. How is that support?

A. I'll call up and they'll sit with me for about 30 minutes and walk me through one exploit. I mentioned to the engineer that it would be great to capture this session and share it with somebody else. And they're starting to do that in 15 to 30-minute sessions.

It's helped me conjure other questions as I see how they did it compared to how I've done it before and a lot of time they have better ideas. I think it's all about being creative. How creative can you be? And this tool allows you to do that.

***“CORE engineers are very, very sharp, very, very savvy.”***

Q. How do you feel about CORE IMPACT overall?

A. I've given a couple of presentations at security roundtables with end user IT administrators and I show them how to exploit vulnerabilities they think are patched. You read about it, you patch your systems, great. Well how can that vulnerability be

exploited? I showed them with a tool like this, how easy it is for a hacker to do that. I like the tool, not so much from an assessment point of view but from a security awareness aspect, making the administrators see how easily this can happen.

Q. And have they embraced the knowledge?

A. Oh, absolutely. It's a two-pronged approach. The first one is how cool CORE IMPACT is, but more importantly it's, "Wow, so that's what that vulnerability is, that's how it's exploited, oh, I see now, okay. So this is why Microsoft is rated as a high security vulnerability or security alert, this is why." I found the tool is really good for system applications, not so much for Web assessment. There are other tools that can do that better than CORE IMPACT.

SANS Bottom Line on CORE IMPACT  
at the Commonwealth of Pennsylvania

1. Easily identifies configuration problems or missing patches;
2. Penetrates network to show true impact of vulnerabilities and avoid false positive problem of standard vulnerability testing;
3. Smooth implementation;
4. Automation feature accomplishes more in a shorter period of time;
5. Shows whether security processes and programs are working;
6. Responsive tech support.

*WhatWorks is a user-to-user program in which security managers who have implemented effective Internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know more about? Let us know. Visit <http://www.sans.org/whatworks> for more information.*